FORESCOUT

Forescout

Security Policy Templates

Configuration Guide

Version 20.0.13

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2020-12-22 10:41

Table of Contents

About Security Policy Templates

Security Policy Templates is a Content Module that uses existing Forescout functionality to detect, evaluate and respond to vulnerabilities and threats - speeding and simplifying your network response. When this module is installed, these templates are available in the Policy view of the Console under the *Vulnerability and Response* sub-folder in the *Templates* tree. Security Policy Templates are named according to the format - *VR <vulnerability name>*. To work with these templates, it is recommended to:

- Read the release notes and review policy logic in the Console's Policy view.
- Enable/add mitigation actions to generated policies.

For more information about Forescout policies, refer to Policy Management in the Forescout Administration Guide.

Third Party Tools

Third party tools are used together with the Security Policy Templates. The tools are provided as is by the individual vendors and are licensed by the respective owners of the software. The individual licensing terms and conditions can be viewed in your CounterACT device at the following location:
`/usr/local/forescout/plugin/spt/documents`

How to Work with the Security Policy Templates Module

This topic describes how to work with the plugin.

What to Do

1. Verify that you have met system requirements. See Security Policy Templates Requirements.
2. Verify the following:
   a. A Primary Classification policy is running on relevant endpoints.
   b. The **Add to Group** actions in the classification policy are enabled.
3. Install the Security Policy Templates Module.

Useful Tools and Best Practices

- To benefit from the updated policy templates provided in this release, remove previously created policies from the Forescout platform and create and activate new policies based on this release.
- Track Vulnerable and Infected Endpoints
- Use Statistics and Status Reports to track the status of policies you create.
- Review and understand the detection/logic model provided by Forescout in these templates before you add or edit rules, or make more extensive customizations.

Security Policy Templates Requirements

The following are requirements for running the Security Policy Templates Module:

- Forescout Windows Vulnerability DB Content Module 18.0.5 or above. It is recommended to have the latest version installed and running. For information about Windows vulnerability DB and how to download it refer to the Windows Vulnerability Content Module Configuration Guide.
- To run policy actions on endpoints with SecureConnector installed, SecureConnector must be running as a service. When using the *Potentially Vulnerable - Latest Security Patches Not Installed* sub rule on endpoints with dissolvable SecureConnector installed, it is recommended to run SecureConnector as an administrator. For more information on SecureConnector refer to Working with SecureConnector in the HPS Inspection Engine
- To run policy actions on endpoints with Remote Inspection, the user must have administrator privileges. For more information and instructions on how to do this refer to Configure Remote Inspection in the HPS Inspection Engine Configuration Guide.
- If you are working with CounterACT 7.0.0:
  - An active Maintenance Contract for CounterACT devices
  - Service Pack 3.0.0 or above

Requirements for Individual Templates

In addition to the requirements listed above, some of the policy templates require these Forescout components:

- These Forescout Network Module plugins must be running:
  - Wireless Plugin
  - VPN Concentrator Plugin
  - Switch Plugin
- These Forescout Endpoint Module plugins must be running:
  - Linux Plugin
  - OS X Plugin
- These Core Extensions Module plugins must be running:
  - Advanced Tools Plugin
  - NBT Scanner
- The *Device Profile Library* Content Module, either:
  - 19.1.11 or above (if you are working with Forescout 8.1 and above)
  - Or 19.0.11 or above (if you are working with CounterACT 8.0.1)

See Policy Templates included in the Security Policy Templates Module for additional individual policy template requirements.

Compatibility

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Install the Security Policy Templates Module

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Flexx Licensing Mode***

   To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download the module **`.fpi`** file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **`.fpi`** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

   The installation begins immediately after selecting Install and cannot be interrupted or canceled.

   In modules that contain more than one component, the installation proceeds automatically one component at a time.
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

Useful Tools for Security Policy Templates

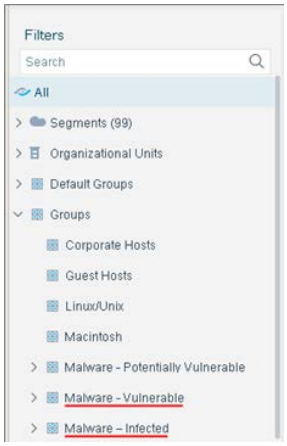
This section describes useful tools for working with the Security Policy Templates module:

- Track Vulnerable and Infected Endpoints
- Statistics and Status Reports

Track Vulnerable and Infected Endpoints

In addition to the actions applied by these policies, it is often useful to identify infected and vulnerable endpoints for further tracking and handling. To do this, the module creates standard folders in the Groups tree of the Filters pane of Home and Asset Inventory views.

Security Policy Templates use the **Add to Group** action to assign endpoints to the Malware-Vulnerable and Malware-Infected groups.



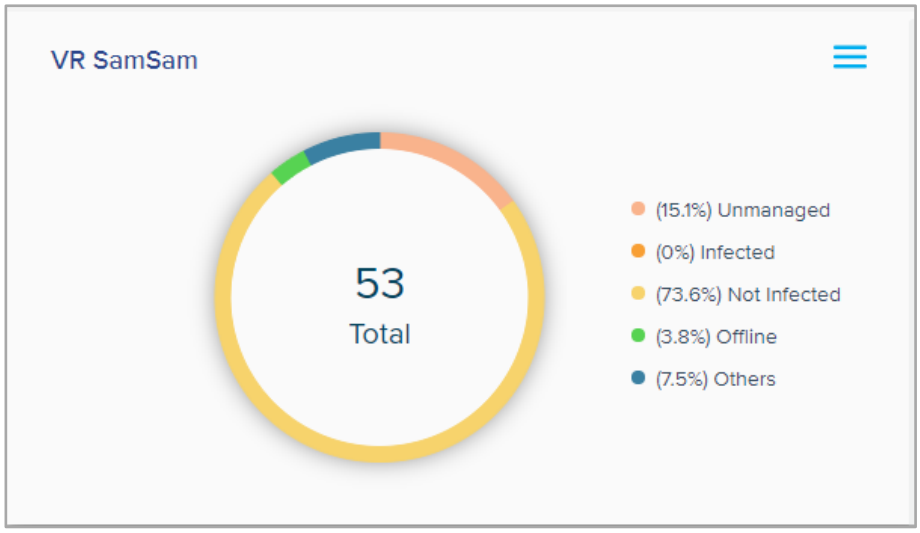
Statistics and Status Reports

This section describes tools that help you track the status of security policies you create.

- Policy Dashboard Widgets
- Testing Policies

Policy Dashboard Widgets

The Dashboard automatically creates a new widget for each installed Security Policy Template. The widget reports the current discovery status of the policy.

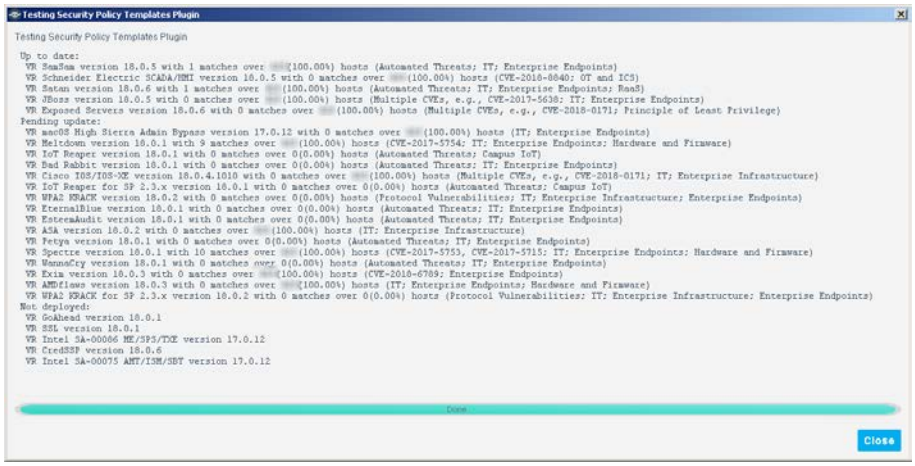


Testing Policies

The Security Policy Templates module includes a Test option that generates a report of the security policy templates that are installed and statistics of the number of matches found for each policy.

To test the Security Policy Templates:

1. Navigate to **Tools > Options > Modules > Security Policy Templates**.
2. Select **Test**.



Policy Templates included in the Security Policy Templates Module

This section provides details of all security policy templates provided in the latest release of the Security Policy Templates Module. In the Policy creation wizard, these templates are installed under the *Vulnerability and Response* sub-folder in the Templates tree.

The Security Policy Templates release are cumulative. **Each module release includes all templates released previously,** as well as all other previous updates and fixes.

Templates released or updated as part of 20.0.13

- VR SolarWinds Orion

Templates released or updated as part of 20.0.12

- VR Amnesia33

Templates released or updated as part of 20.0.9

- VR Zerologon

Templates released or updated as part of 20.0.7

- VR Ripple20
- VR Ripple20 Vulnerability Scanner

Templates released or updated as part of 20.0.4

- VR Zoom

Templates released or updated as part of 20.0.3

- VR SMB Ghost

Templates released or updated as part of 20.0.2

- VR CDP

Templates released or updated as part of 20.0.1

- VR Citrix
- VR CryptoAPI

Templates released or updated as part of 19.0.12

- VR DTEN
- VR Jira
- VR UPnP Servers

Templates released or updated as part of 19.0.11

- VR Google Chrome
- VR PHP

Templates released or updated as part of 19.0.10

- VR Cisco IOS and IOS XE

Templates released or updated as part of 19.0.9

- VR Exim

Templates released or updated as part of 19.0.7

- VR MDS
- VR RingCentral Meetings

Templates released or updated as part of 19.0.6

- VR BlueKeep

Templates released or updated as part of 19.0.5

- VR Cisco ACI
- VR Cisco ASA

Templates released or updated as part of 19.0.4

- VR Apache
- VR PAN GlobalProtect

Templates released or updated as part of 19.0.3

- VR Mirai

Templates released or updated as part of 19.0.2

- VR Cisco RV

Templates released or updated as part of 18.0.12

- VR VMWare Workstation/Fusion

Templates released or updated as part of 18.0.11

- VR BLEEDINGBIT
- VR BLEEDINGBIT OAD

Templates released or updated as part of 18.0.10

- VR Git

Templates released or updated as part of 18.0.8

- VR Foreshadow
- VR Meltdown
- VR Spectre

Templates released or updated as part of 18.0.7

- VR VPNFilter Malware

Templates released or updated as part of 18.0.6

- VR CredSSP
- VR Exposed Servers
- VR Satan

Templates released or updated as part of 18.0.5

- VR JBoss
- VR SamSam
- VR Schneider Electric SCADA/HMI

Templates released or updated as part of 18.0.3

- VR AMDflaws

Templates released or updated as part of 18.0.2

- VR WPA2 KRACK

Templates released or updated as part of 18.0.1

- VR Bad Rabbit
- VR EsteemAudit
- VR EternalBlue
- VR GoAhead
- VR IoT Reaper
- VR Petya
- VR SSL Vulnerability
- VR WannaCrypt/WannaCry

Templates released or updated as part of 17.0.12

- VR Intel SA-00075 AMT/ISM/SBT
- VR Intel SA-00086 ME/SPS/TXE
- VR macOS High Sierra Admin Bypass

VR AMDflaws

Security Policy Templates 18.0.3 or above

Multiple vulnerabilities have been discovered in the AMD Ryzen and EPYC processor lines that include manufacturer backdoors in some chipsets and could allow attackers to gain direct access to the CPU. As a result, an attacker could inject persistent malware in the CPU as well as gain access to and steal network credentials.

For more information, see https://amdflaws.com.

The policies you create with this template detect managed Windows, Linux/Unix and OS X endpoints with the AMD flaws vulnerability.

Requirements

These Forescout Endpoint Module plugins must be running:

- Linux Plugin
- OS X Plugin

VR Amnesia33

Security Policy Templates 20.0.12 or above

CounterACT 8.0.0 or above

Forescout has discovered and disclosed a set of 33 vulnerabilities, which potentially affect millions of devices that utilize any of these four very popular open source TCP/IP stacks:

- uIP
- FNET
- picoTCP
- Nut/Net

TCP/IP stacks affected by Amnesia33 can be found in the operating systems of embedded devices, systems-on-a-chip, networking equipment, OT devices, and a myriad of consumer and enterprise IoT devices.

> *Four of the vulnerabilities received a* **critical** CVSS 3.x Severity Rating *score. Potential impact includes Remote Code Execution, Denial of Service, and exposure of sensitive information.*

Like the *URGENT/11* and the VR Ripple20 and VR Ripple20 Vulnerability Scanner vulnerabilities, this vulnerability affects embedded TCP/IP stacks. But unlike those vulnerabilities, it affects numerous open source stacks that are not owned by a single company. This allows a malicious instance to spread easily and silently across multiple codebases, development teams, companies, and products. This presents significant challenges to patch management.

Policies you create with this template use passive and active techniques, such as HTTP parsing (via Active Inspection or SPAN), DHCP fingerprinting (via IP-helper or SPAN), TCP fingerprinting (via Active Inspection or SPAN), device vendor lookup, NMAP and ICMP, to detect vulnerable and potentially vulnerable devices.

For sensitive environments, such as medical IoTs, passive-only techniques can be used. For smaller remote sites that often cannot provide SPAN traffic, other passive and active techniques are available for full visibility into vulnerable and potentially vulnerable devices across all parts of the network.

Both managed and unmanaged endpoints are evaluated. No credentials are required.

Requirements

- These policies use active inspection methods. Make sure to whitelist all scans originating from the Forescout platform in your next generation firewall, antivirus, or any other similar software.
- The Forescout Core Extensions Module *Advanced Tools Plugin* must be running.

Limitations

- This policy might result some false positives and/or false negatives.

- If you are working with Forescout 8.2.1, *CounterACT Script Result* conditions that generate traffic might fail. This issue affects VR Ripple20, VR Ripple20 Vulnerability Scanner, and VR Amnesia33. For assistance, contact your Forescout sales representative.

Best Practices

It is recommended to do the following:

- Use this policy to detect all vulnerable and potentially vulnerable devices throughout your *entire* network.
- Make sure you are running the latest Forescout eyeSegment Module on your device and segment vulnerable and potentially vulnerable devices discovered by your VR Amnesia33 policy. When creating these segments, consider the business function of each device, as you might want to utilize different mitigation actions based on these differences.
- Use *eyeSegment* and *eyeControl* actions to detect and block anomalous IP traffic.
- Apply segmentation controls to decrease the communication allowed to and from vulnerable and potentially vulnerable devices, thereby limiting the damage done if your network is compromised.
- Monitor traffic to and from high-risk devices continuously. Use eyeSegment to monitor ongoing behavior of devices, and automize the enforcement of more stringent controls to be triggered by the detection of anomalous traffic flow.
- For OT networks, use the newly released *(eyeInspect) SD script* which provides custom detection of active exploitation of these vulnerabilities. Contact your OT representative, SE, or PS engineer to obtain the script.

VR Apache

Security Policy Templates 19.0.4 or above

Requires Core Extensions Module 1.1 or above (Forescout 8.1 or above)

Multiple vulnerabilities have been discovered in the Apache HTTP server. In addition, some versions of Apache have reached End-of-Life.

Policies you create with this template detect managed and unmanaged hosts that run vulnerable or outdated versions of the Apache HTTP server. Endpoints are sorted into Forescout groups based on their level of vulnerability and detected version of Apache. Apply further tests or appropriate remediation actions to each group.

Currently the policy handles Apache releases up to 2.4.39. For details of fixed vulnerabilities, refer to: https://httpd.apache.org/security/vulnerabilities_24.html

Deployment Notes

- This policy uses active inspection methods to resolve endpoint properties. The policy may not evaluate endpoints in the *Properties - Passive Learning* group.
- Detection is more efficient in deployments that use Port Mirroring.

VR Bad Rabbit

Security Policy Templates 18.0.1 or above

Policies based on the following template can help you detect and mitigate Bad Rabbit ransomware (a variant of Petya malware).

Policies you create with this template evaluate whether the endpoints in the policy scope are vulnerable to Bad Rabbit ransomware. Endpoints not yet infected can be "vaccinated" by running a VBS script on the endpoint that creates a file which prevents infection.

- This policy only evaluates endpoints managed by Remote Inspection or SecureConnector.
- The Forescout platform must have permission to run a VBS script in the Windows/system root directory (%windir%).

VR BLEEDINGBIT

Security Policy Templates 18.0.11 or above

CounterACT 8.0 and above

Two chip-level vulnerabilities have been discovered that could impact access points and other unmanaged devices that utilize BLE (Bluetooth Low Energy) chips made by Texas Instruments (TI).

The first vulnerability, BLEEDINGBIT, described in CVE-2018-16986, impacts Cisco and Meraki Access Point devices that use TI BLE chips.

The policies you create with this template classify wireless Access Points and devices connected by WiFi according to their BLEEDINGBIT vulnerability.

VR BLEEDINGBIT OAD

Security Policy Templates 18.0.11 or above

Two chip-level vulnerabilities have been discovered that could impact access points and other unmanaged devices that utilize BLE (Bluetooth Low Energy) chips made by Texas Instruments (TI).

The second vulnerability, BLEEDINGBIT OAD, described in Aruba Networks, impacts the over the air firmware download (OAD) feature of TI chips used in Aruba Wi-Fi access point Series 300 systems.

The policies you create with this template classify wireless Access Points and devices connected by WiFi according to their BLEEDINGBIT OAD vulnerability in the over the air firmware download feature of the device.

Limitations

- Detection of potential vulnerability is not supported for the following Aruba models:
  - AP-3xx and IAP-3xx series access points
  - AP-203R
  - AP-203RP
- The ArubaOS Controller is detected as potentially vulnerable.

VR BlueKeep

Security Policy Templates 19.0.6 or above

The policies you create with this template detect infrastructure devices that are vulnerable or potentially vulnerable to the following exploit: CVE-2019-0708

Both managed and unmanaged endpoints are evaluated. No credentials are required to access endpoints.

Requirements

- Because these policies use active inspection methods, make sure to whitelist all scans originating from the Forescout platform in your next generation firewall, antivirus, and any similar software.
- By default, the policy scope includes all endpoints classified by the Forescout platform as Windows devices, as well as any devices detected as having open RDP ports. To identify these endpoints, apply a Primary Classification or Asset Classification policy and make sure that the Add to Group action is enabled.

VR CDP

Security Policy Templates 20.0.2 or above

CounterACT 8.0.1 or above

Five critical vulnerabilities have been discovered in the Cisco Discovery Protocol (CDP), exposing Cisco devices to Denial-of-service (DoS) attacks and remote code execution. These vulnerabilities affect Cisco switches, Cisco routers, Cisco IP phones, and Cisco IP cameras.

For more information see:

- CVE-2020-3110
- CVE-2020-3111
- CVE-2020-3118
- CVE-2020-3119
- CVE-2020-3120

Policies you create with this template use active inspection methods to detect *vulnerable* or *potentially vulnerable* infrastructure and endpoint devices.

Credentials are required for managed switches and routers.

Requirements

These Forescout components must be running:

- The Endpoint Module *Switch Plugin*
- The Core Extensions Module *Advanced Tools Plugin*
- The *Device Profile Library* Content Module, either:
  - 19.1.10 or above (if you are working with Forescout 8.1 and above)
  - Or 19.0.10 or above (if you are working with CounterACT 8.0.1)

Limitations - False Positives

This policy template detects that a device has been mitigated by disablement of the CDP only if the following criteria is met:

- The device is a managed Cisco switch with an IPv4 address.
- The Appliance that manages the switch is also the Appliance that the switch IP is assigned to.

Other devices that were mitigated by disablement of CDP will be detected as potentially vulnerable, although they are not.

VR Cisco ACI

Security Policy Templates 19.0.5 or above

Policies you create with this template detect potentially vulnerable devices that run Application Centric Infrastructure (ACI) Mode switch software.

The policies you create with this template detect infrastructure devices that are vulnerable or potentially vulnerable to the following exploit:

- Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Default SSH Key Vulnerability (CVE-2019-1804) Cisco_CVE-2019-1804

VR Cisco ASA

Security Policy Templates 19.0.5 or above

Policies you create with this template detect potentially vulnerable devices that run Cisco Adaptive Security Appliance (ASA) software.

The policies you create with this template detect infrastructure devices that are vulnerable or potentially vulnerable to known exploits, in particular:

- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software VPN SAML Authentication Bypass Vulnerability Cisco_CVE-2019-1714
- Cisco Adaptive Security Appliance Software VPN Denial of Service Vulnerability Cisco_CVE-2019-1705

When you update ASA software on endpoints, published fixes for known vulnerabilities are installed. This includes vulnerabilities resolved by the previous version of this template (18.0.2). The following page lists known vulnerabilities in previous ASA software releases: Cisco-Security-Advisories-Responses-and-Notices

Policy logic does not identify endpoints that run Cisco Firepower Threat Defense (FTD) software.

Requirements

- The Forescout Network Module *VPN Concentrator Plugin* must be running.

VR Cisco IOS and IOS XE

Security Policy Templates 19.0.10 or above

Cisco IOS Software and Cisco IOS XE Software vulnerabilities could allow an attacker to cause a remote code execution (RCE) resulting in a denial of service (DoS) condition, or allow the execution of arbitrary code on an affected device.

The policies you create with this template detect potentially vulnerable infrastructure devices with all versions of Cisco IOS and IOS XE software installed. Once vulnerable devices are detected, you should upgrade to the latest fixed software version. This policy evaluates configured Cisco Switch devices.

The 50 latest Cisco IOS/IOS XE vulnerabilities with high or critical severity are recorded. The vulnerability list is automatically updated daily so that vulnerability data is available in the policy template within 24 hours. There is no need to update or refine the policy.

*Switches that are configured as **Not a Switch** are not detected as vulnerable.*

Requirements

- All CounterACT Appliances must have internet access to query the Cisco IOS Software Checker service.
- These Forescout Network Module plugins must be running:
  - Wireless Plugin
  - Switch Plugin

VR Cisco RV

Security Policy Templates 19.0.2 or above

The policies you create with this template detect vulnerable infrastructure devices in the Cisco RV 320 product series.

Policies you create with this template detect vulnerable devices as described in CVE-2019-1653. Vulnerable devices are placed in the Cisco RV - Vulnerable Infrastructure group. Upgrade these devices to the latest fixed software version.

VR Citrix

Security Policy Templates 20.0.1 or above

A vulnerability has been discovered which lets attackers perform directory traversal and code execution on the Citrix Application Delivery Controller (ADC) web server. Citrix ADC (formerly known as *NetScaler*) is a load balancer used for web, application, and database servers. For more information see CVE-2019-19781.

Policies you create with this template use active inspection methods to detect vulnerable or potentially vulnerable Citrix servers. This policy evaluates both managed and unmanaged devices. No credentials are required.

Requirements

- HTTPS access to Citrix severs

VR CredSSP

Security Policy Templates 18.0.6 or above

Credential Security Support Provider protocol (CredSSP) is an authentication provider that processes authentication requests for other applications and is commonly used in RDP (Remote Desktop Protocol) and WinRM (Windows Remote Management).

A remote code execution (RCE) vulnerability exists in unpatched versions of CredSSP. An attacker who successfully exploits this vulnerability could relay user credentials to execute code on the target system. Any application that depends on CredSSP for authentication may be vulnerable to this type of attack.

See blog.preempt.com/security-advisory-credssp and CVE-2018-0886 for more information.

Policies you create with this template detect managed Windows endpoints with the CredSSP vulnerability.

Requirements

- Windows Vulnerability DB 18.0.5 or above

Limitations

- Windows managed endpoints with port 80 or 443 open may be reported as having WS Management when in fact the PowerShell may be not available or may be using a different port.
- For machines running Windows 10 Version 1511, refer to the FAQ section in MSRC-CVE-2018-0886 for guidelines.

VR CryptoAPI

Security Policy Templates 20.0.1 or above

A vulnerability in the CryptoAPI cryptographic library used by Windows operating systems (Crypt32.dll) has been discovered. This vulnerability lets attackers spoof

Elliptic Curve Cryptography (ECC) certificates, allowing them to present malicious executables as if they have come from a trusted source. This also makes the system vulnerable to man-in-the-middle attacks, allowing attackers insight into how to gain access to even more sensitive information on your system.

This vulnerability affects the cryptographic libraries of:

- Windows 10
- Windows Server
- Windows Server 2016
- Windows Server 2019

For more information see NVD-CVE-2020-0601 or MSRC-CVE-2020-0601.

Policies you create with this template ensure that CryptoAPI correctly validates ECC certificates on your MS Windows managed endpoints.

This policy only evaluates MS Windows managed endpoints.

This policy is only necessary if you have decided not to use the recommended Windows Update Compliance v2 Template. For more information about the Windows Update Compliance v2 Template refer to the latest *Forescout Windows Vulnerability DB Configuration Guide.*

Requirements

- If you are using Remote Inspection, endpoint credentials are required. Alternatively, you can use SecureConnector as your inspection method. For more information about SecureConnector refer to the HPS Inspection Engine Configuration Guide.

Limitations

- VR CryptoAPI recognizes endpoints as *patched* if the update was downloaded and installed. However, in some cases the patch might not be active until the endpoint is rebooted. This means that some endpoints might appear as *patched* before the patch is active.

VR DTEN

Security Policy Templates 19.0.12 or above

Requires CounterACT 8.0 and above

Forescout Research Labs have discovered and disclosed multiple vulnerabilities in video conferencing systems manufactured by DTEN (or "DisplayTen"). For more information and mitigation action item recommendations see these articles: forescout.com/company/blog/dten-vulnerability/ and wired.com/story/dten-video-conferencing-vulnerabilities/.

These vulnerabilities affect DTEN interactive touch board modules D5 and D7 that are running DTEN firmware versions 1.3.4 or older. These systems are commonly used as touchscreen smart-TVs or collaborative, real-time whiteboards during Zoom meetings.

These vulnerabilities were given the following identifiers:

- CVE-2019-16270
- CVE-2019-16271
- CVE-2019-16272
- CVE-2019-16273
- CVE-2019-16274

Policies you create with this template detect vulnerable or potentially vulnerable DTEN TVs and whiteboards. The template also includes optional control actions to mitigate risk.

> *This policy was written quite broadly with the intent to catch as many vulnerable and potentially vulnerable endpoints as possible. If you find you are receiving too many false positives, consider adding further classifications to your policy.*

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

Requirements

- The *Device Profile Library* Content Module, either:
  - 19.1.11 or above (if you are working with Forescout 8.1 and above)
  - Or 19.0.11 or above (if you are working with CounterACT 8.0.1)
- To improve traffic inspection, it is recommended to enable these traffic inspection methods:
  - Packet Engine
  - DHCP Classifier
  - Flow Collector (or NetFlow Plugin)

VR EsteemAudit

Security Policy Templates 18.0.1 or above

Policies based on the following template can help you detect and mitigate the EsteemAudit exploit, which targets Windows endpoints:

Policies you create with this template use properties related to installed Windows files to evaluate a Windows endpoint's vulnerability to EsteemAudit malware, and whether Microsoft patches were installed on the endpoint.

> *This policy evaluates all endpoints classified by the Forescout platform as Windows devices.*

VR EternalBlue

Security Policy Templates 18.0.1 or above

Policies based on the following template can help you detect and mitigate malware that exploits the Eternal Blue vulnerability, such as the WannaCry malware package. Typically, Windows endpoints are targeted.

> *See additional policies that detect specific malware packages such as WannaCrypt/WannaCry.*

Policies you create with this template run a script on the Forescout platform which remotely evaluates whether the endpoints in the policy scope are vulnerable to malware that exploits the Eternal Blue vulnerability (MS17-010), such as the WannaCry malware package.

- This policy evaluates all endpoints classified by the Forescout platform as Windows devices.
- This policy evaluates both managed and unmanaged endpoints.
- Analysis of SMB responses may not yield a conclusive result on some endpoints.

VR Exim

Security Policy Templates 19.0.9 or above

Exim is an email server agent used in Unix-like operating systems. This policy template addresses several vulnerabilities in Exim. For example, attackers can send handcrafted messages to exploit buffer overflows resulting with remote code execution (RCE).

This policy template is an extension of the previous VR Exim Policy Template (18.0.3). Vulnerabilities are described in CVE-2019-15846 , CVE-2019-10149, and CVE-2018-6789.

> *If you are upgrading from the previous template version, to safeguard existing functionality, check for actions that have been added or other modifications made to the previous policy based on this template, redeploy the policy, and then re-apply these changes.*

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

VR Exposed Servers

Security Policy Templates 18.0.6 or above

Networks that are exposed to open internet traffic can be vulnerable to attack. Using packet engine SPAN monitoring, the Forescout platform can identify traffic from routable internet addresses, or via well know ports that have been identified as vulnerable.

The policies you create with this template detect traffic seen on the SPAN port to evaluate whether a network segment is exposed to internet traffic. The policy template includes definitions for identifiable ports that are classified as potentially

vulnerable. Users can customize the policy rules to add or exclude ports, server addresses, or IP address ranges.

By default, the untrusted domain is defined as all routable IP addresses.

Requirements

- A Packet Engine with SPAN for monitoring traffic from the internet

Limitations

- 123/UDP and ports higher than 1024/UDP are excluded to prevent false positives.
- IPv4 network addresses only.

VR Foreshadow

Security Policy Templates 18.0.8 or above

Foreshadow is a speculative execution attack on Intel processors which allows an attacker to steal sensitive information stored inside personal computers or third-party clouds. Foreshadow has two versions:

- An attack designed to extract data from SGX enclaves.
- A Next-Generation version which affects Virtual Machines (VMs), hypervisors (VMM), operating system (OS) kernel memory, and System Management Mode (SMM) memory.

For more information, see foreshadowattack.eu and also: CVE-2018-3615, CVE-2018-3620, and CVE-2018-3646.

The policies you create with this template detect managed Windows, Linux/Unix and OS X endpoints with the Foreshadow vulnerability.

This policy provides customized third-party detection tools. Some tools such as Anti-Virus applications may prevent the policy from working properly. You may need to manually whitelist the *fs_test_SpeculationControl.bat* and *fs_test_pti_Linux.sh* executables used in the Expected Script Results conditions.

Requirements

- Windows PowerShell scripts must be allowed to run on Windows managed endpoints running Windows 7/Windows 20XX Server or above.

VR Git

Security Policy Templates 18.0.10 or above

Several vulnerabilities have been discovered in the Git Project that allow an attacker to execute arbitrary code during processing of a recursive "git clone".

For more information, see CVE-2018-11235 and CVE-2018-17456.

The policies you create with this template detect managed Windows, Linux/Unix, and OS X end points with the Git vulnerability.

Some tools such as Anti-Virus applications may prevent this policy from working properly. You may need to manually whitelist the *fs_test_git_Linux.sh* and *fs_test_git_Mac.sh* executables used in the Expected Script Results conditions.

VR GoAhead

Security Policy Templates 18.0.1 or above

GoAhead httpd 2.5 < 3.6.5, also known as LD_PRELOAD exploit (CVE-2017-17562), is a vulnerability found in the GoAhead web server software in IoT devices that allows remote code execution (RCE) that can be potentially remotely exploited to hijack gadgets.

This policy identifies potentially vulnerable devices and by applying control may be used proactively to prevent security breaches, data leakage and DDoS attacks.

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

VR Google Chrome

Security Policy Templates 19.0.11 or above

Policies you create with this template detect endpoints running vulnerable versions of the Google Chrome browser. Vulnerabilities in these versions can be exploited by hackers to execute code remotely.

This policy template is an extension of previous VR Google Chrome Policy Templates (19.0.9). Vulnerabilities are described in Google release information for November 6th 2019.

> *If you are upgrading from the previous template version, to safeguard existing functionality, check for actions that have been added or other modifications made to the previous policy based on this template, redeploy the policy, and then re-apply these changes.*

Update the Google Chrome browser on the relevant endpoints to a stable release.

Requirements

These Forescout Endpoint Module plugins must be running:

- Linux Plugin
- OS X Plugin

To run scripts on managed endpoints:

- If necessary, manually whitelist the **`fs_test_chrome_Linux.sh`** executable used in policy conditions.

VR Intel SA-00075 AMT/ISM/SBT

Security Policy Templates 17.0.12 or above

The policies you create with this template detect Windows and Linux/Unix endpoints with Intel SA-00075 AMT/ISM/SBT vulnerability.

This policy only detects vulnerabilities on managed endpoints. This policy provides a third-party Intel detection tool. Linux endpoint or server support includes Ubuntu 16.04 LTS and 14.04 LTS or higher.

- *Some tools such as Anti-Virus may prevent the policy from working properly. If this happens, you may need to manually whitelist the "fs_test_00075.exe" and "fs_test_00075_Linux.sh" executables used in the Expected Script Results conditions.*

- *The tool does not support Virtual Machine (VM) environments.*

Requirements

- The Forescout Endpoint Module *Linux Plugin* must be running

Windows endpoints/servers:

- Microsoft Windows 7, 8, 8.1, or 10
- Local operating system administrative access

Linux endpoints/servers:

- Ubuntu 16.04 LTS and 14.04 LTS.
- Local operating system administrative access
- The Intel® Management Engine Components, specifically: The Intel® Management Engine Interface driver (Intel® MEI).

VR Intel SA-00086 ME/SPS/TXE

Security Policy Templates 17.0.12 or above

The policies you create with this template detect Windows and Linux/Unix endpoints with Intel SA-00086 ME/SPS/TXE vulnerability.

This policy only detects vulnerabilities on managed endpoints. This policy provides a third-party Intel detection tool.

- *Some tools such as Anti-Virus may prevent the policy from working properly. If this happens, you may need to manually whitelist the "fs_test_00086.exe" and "fs_test_00086_Linux.sh" executables used in the Expected Script Results conditions.*

Requirements

- The Forescout Endpoint Module with the Linux Plugin running

Windows endpoints/servers:

- Microsoft Windows* 7, 8, 8.1, or 10 (Windows* 10S and Windows*10 IOT Core are not supported)
- Windows* 2012 R2 for servers (x64)
- .NET Framework 4.5 or higher
- HECI Driver
- Local operating system administrative access

Linux endpoints/servers:

- Python 2.7 or higher
- Ubuntu LTS 16.0.4 (for client), Redhat 7.2 (for Server)
- Local operating system administrative access

VR IoT Reaper

Security Policy Templates 18.0.1 or above

Policies based on the following templates use Forescout remote scanning capabilities to evaluate IoT device vulnerability to the ports and HTTP protocols used by the botnet for download and infection.

The VR IoT Reaper policy and VR IoT Reaper for SP 2.3.x policy should not be used together in the same system.

This policy scans potentially vulnerable IoT devices for vulnerable ports. Once such a device is detected, the Forescout platform tests these ports with the HTTP protocol that is used by the botnet for infection. Suspected vulnerable devices are reported by the Forescout platform.

Requirements

- Your system must be running the Primary Classification policy to work with this template.

VR JBoss

Security Policy Templates 18.0.5 or above

CounterACT 8.0 or above

The default configuration of JBoss application servers does not restrict access to the console and web management interfaces, which allows remote attackers to bypass authentication and gain administrative access via direct requests. Once compromised, these servers can be used to distribute malware.

For more information, see blog.talosintelligence.com-jboss-backdoor and CVE-2017-5638.

The policies you create with this template detect JBoss application servers in a local network and perform a JBoss server scan to look for vulnerabilities.

It is recommended to patch the server software to the latest JBoss version.

VR Jira

Security Policy Templates 19.0.12 or above

A logic error in Jira's Whitelisting policies lets attackers access the content of internal network resources by using server-side request forgery (SSRF). For more information see CVE-2019-8451 or jira.atlassian.com-JRASERVER-69793.

Policies you create with this template use active inspection methods to detect Jira servers that are vulnerable to this issue. You can customize this policy to suit your own naming conventions of Jira servers. The policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

VR macOS High Sierra Admin Bypass

Security Policy Templates 17.0.12 or above

The policies you create with this template detect Macintosh endpoints with macOS High Sierra admin bypass vulnerability.

This policy only detects vulnerabilities on managed endpoints.

> *When upgrading from the macOS High Sierra security template version 10.13.0 to 10.13.1, a reboot is required for the patches to complete installation.*

Requirements

- The Forescout Endpoint Module *OS X Plugin* must be running
- To run policy actions on endpoints with Secure Connector installed, Secure Connector must be running as a service
- To run policy actions on endpoints with Remote Inspection, the user must have administrator privileges

By default, the Forescout platform uses the Windows Vulnerability DB to distribute vulnerability information. For more information about download options supported by the Forescout platform, see these sections of the *Forescout Endpoint Module: HPS Inspection Engine Configuration Guide*:

- Distributing Vulnerability Information to Windows Endpoints
- Using Windows Server Update Services (WSUS) or Windows Update
- Windows Update Default Settings

VR MDS

Security Policy Templates 19.0.7 or above

Forescout 8.1.2 or above

Microarchitectural Data Sampling (MDS) exploits, such as the *RIDL* and *Fallout* exploits, take advantage of MDS side-channel vulnerabilities in Intel CPUs to access arbitrary pieces of private information. It is similar to the VR Meltdown and the VR Spectre vulnerabilities. These vulnerabilities are described in mdsattacks.com.

Policies you create with this template detect managed Windows, Linux/Unix, and macOS™/OS X® endpoints that are vulnerable to MDS exploits.

Requirements

- These Endpoint Module plugins must be running:
  - Linux Plugin 1.4.1
    - Make sure the Linux Plugin uses root credentials to access endpoints.
  - OS X Plugin 2.2.1
    - OS X Plugin SecureConnector deployed as a Service.
    - Make sure the OS X Plugin Remote Inspection uses root credentials to access endpoints.
- Policies created with this template provide customized third party detection tools. Make sure the fs_test_SpeculationControl.bat and fs_test_MDS_Linux.sh executables used in the Expected Script Results conditions are whitelisted (Do this manually if needed), so that tools such as Anti-Virus applications do not prevent the policy from working properly.
- Policies created with this template use Windows PowerShell scripts. Make sure that these scripts are allowed on Windows managed endpoints running Windows 7, Windows 2008 Server or above.

VR Meltdown

Security Policy Templates 18.0.8 or above

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system. Meltdown is described in CVE-2017-5754, see meltdownattack.com for more information.

This vulnerability is similar to the VR Spectre and the VR MDS vulnerabilities.

The policies you create with this template detect managed Windows, Linux/Unix and OS X endpoints with the Meltdown vulnerability.

This policy provides a third-party Microsoft detection tool. Some tools such as Anti-Virus applications may prevent the policy from working properly. You may need to manually whitelist the *fs_test_SpeculationControl.bat* and *fs_test_pti_Linux.sh* executables used in the Expected Script Results conditions.

Requirements

- Windows PowerShell scripts must be allowed to run on Windows managed endpoints running Windows 7/Windows 20XX Server or above.

VR Mirai

Security Policy Templates 19.0.3 or above

Policies based on the following template can help you detect and remediate variants of the Mirai botnet.

Policies you create with this template evaluate endpoint vulnerability to a Mirai variant that targets enterprise devices, in particular WePresent WiPG-1000 Wireless Presentation systems and LG Supersign displays. For details, refer to unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems, which links to related exploits.

Vulnerable and potentially vulnerable endpoints are assigned to Forescout groups for further remediation. Based on this evaluation, you can apply controls that proactively prevent security breaches, data leakage, and DDoS attacks.

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

Requirements

- This policy uses the results of Forescout endpoint classification. A primary classification policy must be applied to endpoints.

VR PAN GlobalProtect

Security Policy Templates 19.0.4 or above

Policies based on the following template can help you detect and remediate vulnerabilities in Palo Alto Networks (PAN) GlobalProtect Agent.

Some versions of PAN Global Protect Agent are vulnerable to spoofing. Attackers can replay authentication or session tokens to gain access as the user.

Policies you create with this template detect Windows and OS X endpoints that run vulnerable or outdated versions of the PAN GlobalProtect Agent. Managed and unmanaged endpoints are evaluated. Endpoints are sorted into Forescout groups based on their level of vulnerability and detected software version. Apply further tests or appropriate remediation actions to each group. This vulnerability is described in CVE-2019-1573.

Requirements

- The Forescout Endpoint Modules *OS X Plugin* must be running

Detection is more efficient in deployments that use Port Mirroring.

VR Petya

Security Policy Templates 18.0.1 or above

Policies based on the following template can help you detect and mitigate Petya ransomware.

Policies you create with this template evaluate whether the endpoints in the policy scope are vulnerable to Petya ransomware. Infected endpoints are detected before the terminal reboot phase. Endpoints not yet infected can be "vaccinated" by running a VBS script on the endpoint that creates a file which prevents infection.

> *This policy only evaluates endpoints managed by Remote Inspection or SecureConnector.*

VR PHP

Security Policy Templates 19.0.11 or above

Multiple vulnerabilities have been discovered in PHP. These vulnerabilities allow attackers to execute arbitrary code. Depending on the privileges of the exploited application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of these vulnerabilities can also result in a denial-of-service.

This policy template is an extension of the previous VR PHP Policy Template (19.0.9). The template has been updated to support the current PHP supported versions, detecting "End-of-Life" (EOL) and "Security Only" versions of PHP as well as the latest vulnerabilities for PHP. For more information on PHP version support and the latest vulnerabilities see PHP-supported-versions, cisecurity.org-2019-116 and CVE-2019-11043.

> *If you are upgrading from the previous template version, to safeguard existing functionality, check for actions that have been added or other modifications made to the previous policy based on this template, redeploy the policy, and then re-apply these changes.*

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

VR RingCentral Meetings

Security Policy Templates 19.0.7 or above

Forescout 8.1.2 or above

Some versions of the RingCentral conferencing application are vulnerable to attack. A user can be unknowingly connected to a video call, letting an attacker access the user's device and its video camera. This vulnerability is similar to the VR Zoom vulnerability, also covered in the current Security Policy Templates release.

Policies you create with these templates detect macOS™/OS X® endpoints that run v*ulnerable or outdated versions of RingCentral Meeting*. Managed endpoints are evaluated. Endpoints are sorted into Forescout groups according to their level of

vulnerability and detected software version. Apply further tests or appropriate remediation actions to each group.

This vulnerability is described in CVE-2019-13450 and CVE-2019-13567.

Requirements

- The Forescout Endpoint Module *OS X Plugin* 2.2.1 or above must be running

VR Ripple20

Security Policy Templates 20.0.7 or above

CounterACT 8.0.0 or above

Multiple vulnerabilities have been discovered in a popular TCP/IP stack implementation known as *Treck*. Forescout Research Labs partnered with JSOF and used data from Forescout's unique Device Cloud to identify dozens of vendors that could potentially be affected. These vulnerabilities include *remote code execution*, *Out-of-bounds Write*, and *sensitive data exposure*. For more information and best practices see:

- cve.mitre.org-CVE-2020-11896–CVE-2020-11914 (19 vulnerabilities in total)
- carnegie-mellon-university-vulnerability-note
- Forescout-Blog-identifying-and-protecting-devices-vulnerable-to-ripple20

Policies you create with this template use both passive and active inspection methods to evaluate if devices are *potentially vulnerable*. If the VR Ripple20 Vulnerability Scanner is also running, the VR Ripple20 policies also detect which devices are *vulnerable*. Both managed and unmanaged endpoints are evaluated. No credentials are required to access endpoints.

This policy template is an extension of the previous VR Ripple20 Policy Template (20.0.6).

> *If you are upgrading from the previous template version, to safeguard existing functionality, check for actions that have been added or other modifications made to the previous policy based on this template, redeploy the policy, and then re-apply these changes.*

Caution

Policies created with this template use Nmap scans, including Nmap OS detection scans to detect potentially vulnerable devices. If you have sensitive devices (for example, OT devices) in your environment, and you do not want to expose them to this type of scan, limit the policy scope by adding the sensitive devices to the Passive Learning group. For more information refer to the section on *Passive Management of Sensitive Endpoints* in the *Forescout Operational Technology Module Configuration Guide* and/or the section on the *Passive Learning Mode Template* in the *Forescout Administration Guide.*

Requirements

- These policies use active inspection methods. Make sure to whitelist all scans originating from the Forescout platform in your next generation firewall, antivirus, and any other similar software.
- The Forescout Core Extensions Module *Advanced Tools Plugin* must be running.

Limitations

This policy might result some false positives and/or false negatives.

Best Practices

For optimal performance:

- Ensure proper network hygiene and isolation of highly sensitive information from external contact using the Forescout eyeSegment application and SilentDefense LAN CP (Forescout Operational Technology Module). For more information refer to the *Forescout eyeSegment Application How-to Guide* and the *Forescout Operational Technology Module Configuration Guide.*
- Configure your organization's firewall to allow ICMP MS SYNC traffic (type 165 and 166) to travel to and from CounterACT Appliances.
- Enable DHCPv6 on your CounterACT devices.

  On each CounterACT Appliance:

  a. Run this command: **`fstool dhclass set_property config.enable_reading_dhcpv6_packets.value 1`**

  b. Restart the DHCP Classifier Plugin.

For more information on best practices refer to the Forescout_Blog.

VR Ripple20 Vulnerability Scanner

Security Policy Templates 20.0.7 or above

CounterACT 8.0.0 or above

Multiple vulnerabilities have been discovered in a popular TCP/IP stack implementation known as *Treck*. Forescout Research Labs partnered with JSOF and used data from Forescout's unique Device Cloud to identify dozens of vendors that could potentially be affected. These vulnerabilities include *remote code execution*, *Out-of-bounds Write*, and *sensitive data exposure*. For more information and best practices see:

- cve.mitre.org-CVE-2020-11896–CVE-2020-11914 (19 vulnerabilities in total)
- carnegie-mellon-university-vulnerability-note
- Forescout-Blog-identifying-and-protecting-devices-vulnerable-to-ripple20

This policy template detects devices that are *vulnerable* to the *Ripple20* vulnerabilities, and delivers this information into the *VR Ripple20* policy. Both managed and unmanaged endpoints are evaluated. No credentials are required to access endpoints.

Caution

Policies created with this template send malformed packets to endpoints in order to detect endpoints that are vulnerable to this type of attack. If you have sensitive devices (for example, OT devices) in your environment, and you do not want to expose them to this type of inspection, limit the policy scope by adding the sensitive devices to the Passive Learning group. For more information refer to the section on *Passive Management of Sensitive Endpoints* in the *Forescout Operational Technology Module Configuration Guide* and/or the section on the *Passive Learning Mode Template* in the *Forescout Administration Guide.*

Requirements

- These policies use active inspection methods. Make sure to whitelist all scans originating from the Forescout platform in your next generation firewall, antivirus, and any other similar software.
- The Forescout Core Extensions Module *Advanced Tools Plugin* must be running.
- VR Ripple20 must be running.

Limitations

This policy might result some false positives and/or false negatives.

Best Practices

For additional detection, review the findings of the *VR Ripple20 Vulnerability Scanner* policy and consider enabling the *Add to Group* action in the *Likely Vulnerable* sub-rule, so that *Likely Vulnerable* devices are added to the VR Ripple20 *Vulnerable* sub-rule.

VR SamSam

Security Policy Templates 18.0.5 or above

SamSam is high-risk ransomware designed to infect unpatched servers and encrypt files stored on computers networked to the infected server. This ransomware is distributed manually. Samsam employs the RSA-2048 asymmetric encryption algorithm and, therefore, two keys (public and private) are generated during encryption - public to encrypt, private to decrypt.

For more information, see blog.talosintelligence.com-samsam-ransomware.

The policies you create with this template detect managed Windows endpoints that are infected with the *I am sorry* variant of this malware.

VR Satan

Security Policy Templates 18.0.6 or above

A Ransomware as a Service (RaaS) that distributes the Satan ransomware has been discovered. This service allows any potential attacker to register an account with the

service, and create and distribute their own customized version of the Satan ransomware.

Satan ransomware (discovered in January 2017) targets Windows computers, and encrypts the files on a victim's computer, scrambling the encrypted file names, and appending the *.STN* extension and others to the file name.

See bleepingcomputer.com-new-satan-ransomware-available-through-a-ransomware-as-a-service for more information on the Ransomware as a Service that has been observed in the wild.

The policies you create with this template detect managed Windows endpoints that are infected with the Satan ransomware.

Limitations

In some rare cases, files generated by Windows may result in a false positive indicator for the Satan ransomware.

VR Schneider Electric SCADA / HMI

Security Policy Templates 18.0.5 or above

A significant vulnerability in Schneider Electric Software used at manufacturing and energy facilities could allow hackers to execute arbitrary code and in a worst-case scenario, disrupt or cripple plant operations. An attacker without credentials could use the vulnerability to compromise the security of a machine in a manufacturing or energy production plant, and could move laterally within the organization's network to carry out additional attacks.

The vulnerabilities affect the following Schneider Electric Software:

- InduSoft Web Studio v8.1 and prior versions.
- InTouch Machine Edition 2017 v8.1 and prior versions.

For more information, see software.schneider-electric.com-security-bulletin and CVE-2018-8840.

The policies you create with this template detect vulnerabilities on managed Windows endpoints.

VR SMB Ghost

Security Policy Templates 20.0.3 or above

This vulnerability is also known as *EternalDarkness*.

A critical vulnerability has been discovered in the SMBv3 protocol that can be used for remote code execution attacks on either servers or client devices that are using this connection protocol. This vulnerability can be exploited by hackers to create devastating ransomware campaigns and attacks like the WannaCry attack of May 2017. For more information about the SMB Ghost vulnerability see CVE-2020-0796 or portal.msrc.microsoft.com-security-guidance-adv200005.

Policies you create with this template use active inspection methods to detect *potentially vulnerable* servers and endpoints that are unpatched against this highly

threatening vulnerability. The policy uses the 445/tcp port to query servers and endpoints. No credentials are required.

VR SolarWinds Orion

A supply chain attack targeting SolarWinds® Orion® Platform software was found. Attackers can control compromised endpoints, allowing Remote Code Execution, Denial of Service attacks, and exposure of sensitive information.

Policies you create with this template evaluate both managed and unmanaged Windows endpoints to determine their vulnerability. Policies use passive and/or active inspection methods to evaluate endpoints. No credentials are required to access endpoints.

This vulnerability is tracked as FireEye UNC2452. The policy also detects CVE 2019-9546. Policies created with this template assess vulnerability based on newly identified artifacts and unpatched legacy applications. See the full advisory for details of vulnerable SolarWinds product builds.

For updates about Forescout's response to this threat, see our blog page tracking this issue.

Policy-based Detection

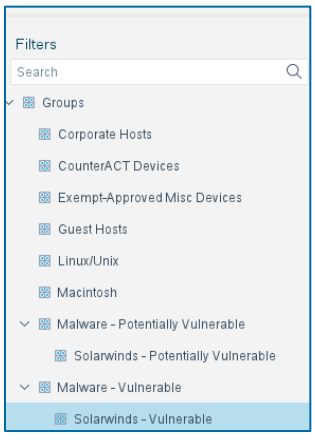
Endpoint vulnerability is determined based on the presence of SUNBURST malware and other suspicious SolarWinds applications and services, related open ports, and other factors.

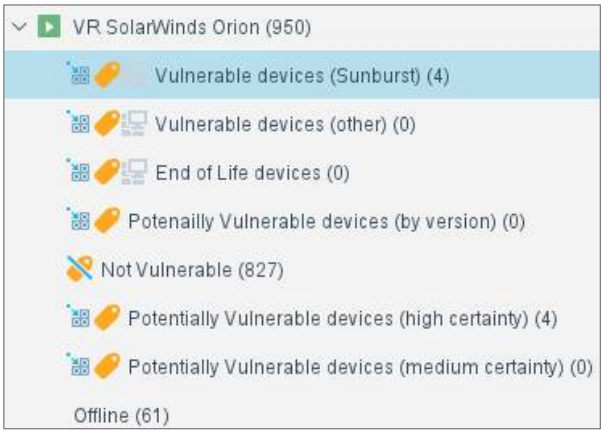
- *To allow detailed inspection of SolarWinds servers, it is strongly recommended to ensure they can be managed using Remote Inspection or SecureConnector. This lets the policy run in-depth inspection scripts on these sensitive endpoints.*

- *As information about this exploit develops, or the attack adapts, modify your policies to search for other application drop/installation locations.*

Remediation of Vulnerable Endpoints

In your Console, endpoints evaluated as *Vulnerable* or *Potentially Vulnerable* are labeled and assigned to *Malware* sub-groups for further handling. In addition, a set of Inventory views break down endpoints by vulnerability in greater detail, reflecting policy rules.





- On endpoints with SolarWinds applications, install patches or hotfixes provided by SolarWinds and/or upgrade to protected builds.

- Review endpoints with SolarWinds services or open ports associated with this exploit to see if these artifacts are legitimately present.
- Optional Virtual Firewall actions in the policy template can be enabled to provide an initial response upon detection.
- Customize your response with other eyeControl actions, and functionality provided by eyeSegment or other Forescout solutions.

The policy populates the following new Inventory views:

Vulnerable devices (Sunburst)	Known SUNBURST malware components detected.
Vulnerable devices (other)	Evidence of compromised SolarWinds components.
End of Life devices	SolarWinds applications that are no longer supported were detected. These builds may have vulnerabilities other than SUNBURST malware, and should be upgraded.
Potentially Vulnerable devices (by version)	Vulnerable SolarWinds application builds detected.
Not Vulnerable	Windows environment and/or SolarWinds applications that are not vulnerable. Non-Windows endpoints are cleared to this group.
Potentially Vulnerable devices (high certainty)	Open communication ports and/or SolarWinds services associated with this exploit were detected.
Potentially Vulnerable devices (medium certainty)	
Offline	Endpoint not available for evaluation.
Other	Endpoint could not be assigned to other groups, or vulnerability could not be evaluated.

Requirements

- CounterACT 8.0.0 or above
- Active inspection methods may be used on some endpoints. Whitelist all scans originating from the Forescout platform in your firewall, antivirus, and any other similar software.
- The Advanced Tools Plugin must be running.

Limitations

This policy may yield some false positives and/or false negatives.

VR Spectre

Security Policy Templates 18.0.8 or above

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre. Spectre is described in

CVE-2017-5753 and CVE-2017-5715, see https://meltdownattack.com for more information.

This vulnerability is similar to the VR Meltdown and VR MDS vulnerabilities.

The policies you create with this template detect managed Windows, Linux/Unix and OS X endpoints with the Spectre vulnerability.

This policy provides a third-party Microsoft detection tool. Some tools such as Anti-Virus applications may prevent the policy from working properly. You may need to manually whitelist the *fs_test_SpeculationControl.bat* and *fs_test_pti_Linux.sh* executables used in the Expected Script Results conditions.

Requirements

- Windows PowerShell scripts must be allowed to run on Windows managed endpoints running Windows 7/Windows 20XX Server or above.

VR SSL Vulnerability

Security Policy Templates 18.0.1 or above

The policies you create with this template detect HTTPS servers that are vulnerable to malware that exploits SSL vulnerabilities in managed and unmanaged endpoints. For example, the ROBOT Attack TLS Decryption Vulnerability (Return of Bleichenbacher's Oracle Threat) and the Heartbleed vulnerability.

The Robot Attack TLS Decryption Vulnerability is a 19-year-old vulnerability that allows performing RSA decryption and signing operations with the private key of a TLS server. For more information on the vulnerability, see eprint.iacr.org/2017/1189 and robotattack.org.

Heartbleed is a serious vulnerability in the OpenSSL cryptographic software library that allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

This policy template can be customized to accommodate different IP address ranges and specific HTTPS ports.

VR UPnP Servers

Security Policy Templates 19.0.12 or above

BCMUPnP_Hunter is a botnet that targets routers that have the Universal Plug and Play (UPnP) Server feature enabled. The botnet takes advantage of a known vulnerability discovered in 2013 and described by Defensecode.com.

BCMUPnP_Hunter is a self-built proxy network, which initially looks like it's being used to push out spam from web mail sources. The botnet then scans the TCP and UDP ports of the targeted device for ways to access the device, and sends an exploit payload to the target.

For more information, see threatpost.com.

This policy template is an extension of the previous VR UPnP Servers Policy Template (18.0.11). The policies you create with this template use Active Scanning to remotely evaluate whether the endpoints and devices in the policy scope have UPnP Servers that are exposed to network traffic. You can customize the policy rules to add or exclude ports, server addresses, or IP address ranges.

> *If you are upgrading from the previous template version, to safeguard existing functionality, check for actions that have been added or other modifications made to the previous policy based on this template, redeploy the policy, and then re-apply these changes.*

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

VR VMWare Workstation/Fusion

Security Policy Templates 18.0.12 or above

Policies you create with this template evaluate managed Windows, Linux, and Mac/OS X endpoints that run VMware Workstation/Fusion to detect vulnerabilities announced by VMware.

This template is new for this version. Currently these evaluations are performed:

- End of Life – endpoints running versions of VMware Workstation/Fusion that are no longer supported.
- Known Vulnerability – vulnerable endpoints as described in VMware security advisory VMSA-2018-0030 (CVE-2018-6983). For details, refer to: vmware.com-VMSA-2018-0030 or CVE-2018-6983

Requirements and Limitations

Windows endpoints must be managed by SecureConnector or by Remote Inspection with an admin user.

For Linux endpoints:

- The Forescout Endpoint Module *Linux Plugin* must be running.
- Endpoints must be managed by SecureConnector or by Remote Inspection with an admin user.
- This policy uses the **Expected Script Results** property, which runs scripts on endpoints. If AntiVirus applications and other tools block these scripts, the policy will not work properly. You may need to manually whitelist the **`fs_test_vmware_Linux.sh`** executable used to resolve the **Expected Script Results** property.

For OS X endpoints:

- The Forescout Endpoint Module *OS X Plugin* must be running.
- OS X endpoints must be managed in one of these ways:
  - OS X SecureConnector deployed as a Service.
  - Remote Inspection by a user that can run scripts with root permissions.

VR VPNFilter Malware

Security Policy Templates 18.0.7 or above

VPNFilter malware is a multi-stage, modular platform with versatile capabilities to support both intelligence collection and destructive cyber attack operations.

- The stage 1 malware persists through a reboot, to gain a persistent foothold and enable the deployment of the stage 2 malware.
- The stage 2 malware (which does not persist through a reboot) possesses capabilities such as file collection, command execution, data exfiltration and device management. Some versions of stage 2 also possess a self-destruct capability that overwrites a critical portion of the device's firmware and reboots the device, rendering it unusable.
- Stage 3 modules serve as plugins for the stage 2 malware, providing stage 2 with additional functionality such as a *packet sniffer* for collecting traffic passing through the device, including theft of website credentials and monitoring of Modbus SCADA protocols, and a *communications module* that allows stage 2 to communicate over Tor.

For more information, see blog.talosintelligence.com-vpnfilter-update.

Policies you create with this template detect potentially vulnerable devices. The policy can be tailored by the operator to specify different ports, or to identify different patterns that indicate vulnerability.

To scan endpoints that are connected through potentially infected devices, you can utilize a third party router testing tool for the VPN Filter malware provided by Symantec: symantec.com-filtercheck

VR WannaCrypt / WannaCry

Security Policy Templates 18.0.1 or above

Policies based on the following template can help you detect and mitigate WannaCrypt/WannaCry ransomware, which targets Windows endpoints.

> *See also the EternalBlue policy template that addresses this vulnerability.*

Policies you create with this template use Forescout properties related to Windows registry keys, running services, and installed files to detect Windows endpoints infected with known variants of WannaCry/WannaCrypt malware.

- This policy only evaluates endpoints managed by Remote Inspection or SecureConnector.
- WannaCrypt malware exploits a vulnerability in SMB connectivity, which was identified by Microsoft and published as technet.microsoft.com-ms17-010 in March 2017.

The policy provided in this release check for this vulnerability as part of endpoint evaluation - and can cause download of Microsoft vulnerability information to Windows endpoints.

VR WPA2 KRACK

Security Policy Templates 18.0.2 or above

Krack is a vulnerability in the WPA2 wireless protocol that could allow attackers to eavesdrop on wireless connections and inject data into the wireless stream in order to install malware or modify web pages.

Policies based on this template classify WiFi connected devices according to KRACK risk, based on the detected software release. Windows managed devices are checked for the Oct 2017 patch. See Remediating WPA2 KRACK on Wireless Controllers and Access Points for details about remediation of Wireless controllers and access points.

The VR WPA2 KRACK policy and VR WPA2 KRACK for SP 2.3.x policy should not be used together in the same system.

Requirements

- The Forescout Network Module *Wireless Plugin* must be running

Remediating WPA2 KRACK on Wireless Controllers and Access Points

Policies based on the VR WPA2 KRACK use the **WLAN Device Software** property provided by the Wireless Plugin to evaluate vulnerability to WPA2 KRACK malware. Risk is assessed based on the software release on the controller.

- ***For Cisco and Aruba controllers***, policy rules identify vulnerable devices based on currently known information about software releases.
  - Add policy actions to remediate devices that were found to be vulnerable.
  - In the Asset Inventory view, examine policy results per rule.
- ***For controllers of other vendors***, follow this procedure:
  a. Create and run a policy based on one of the templates.
  b. The Forescout platform populates the Asset Inventory view for the **WLAN Device Software** property.
  c. In the Asset Inventory view for this property, review the software releases that the Forescout platform detected on your controllers. Refer to manufacturer announcements of vulnerability and patch information for these software releases.
  d. Use the **WLAN Device Software** property in policies you create to detect and remediate devices that run vulnerable software.

VR Zerologon

Security Policy Templates 20.0.9 or above

CounterACT 8.0.1 or above

'Zerologon' (Zero-logon) is an ***extremely high severity vulnerability*** which lets attackers subvert Microsoft Netlogon Remote Protocol (MS-NRPC) cryptographic authentication procedure, thus allowing attackers to rapidly infiltrate your network and:

- Disable security features in the Netlogon authentication process

- Impersonate any computer on your network
- ***Access your domain controllers*** - It is extremely rare and alarming for hackers to gain this type of access.

*This vulnerability received a **'10.0 Critical'** (out of 10) CVSS 3.x Severity Rating.*

For more information on this vulnerability refer to MS-CVE-2020-1472 and kb.cert.org/vuls/id/490028.

Policies you create with these templates use active inspection to detect managed and unmanaged servers running MS-NRPC. These policies inspect all versions of Windows Server (2008 or above). No credentials are required.

Requirements

- These policies use active inspection methods. Make sure to whitelist all scans originating from the Forescout platform in your next generation firewall, antivirus, and any similar software.
- This policy requires knowledge of the NetBIOS hostname of inspected servers. Ensure that the Forescout Core Extensions Module *NBT Scanner Plugin* is running.
- The Forescout Core Extensions Module *Advanced Tools Plugin* must be running.

Best Practices

To speed-up detection of vulnerable endpoints, consider limiting the policy scope to your Domain Controller group(s).

Limitations

This policy template uses a third-party script. False positives and negatives might apply.

VR Zoom

Security Policy Templates 20.0.4 or above

Some versions of the Zoom conferencing application are vulnerable to multiple types of attacks including *Remote Code Execution (RCE)*. Some of these vulnerabilities let attackers access any compromised endpoint's camera and microphone after any Zoom session has ended. Other Zoom vulnerabilities let the attacker gain root access to the compromised endpoint. Another vulnerability lets an attacker decrypt private Zoom session data, exposing valuable information.

This policy template is an extension of the previous VR Zoom Policy Template (19.0.7).

If you are upgrading from the previous template version, to safeguard existing functionality, check for actions that have been added or other modifications made to the previous policy based on this template, redeploy the policy, and then re-apply these changes.

This new policy template continues to cover the vulnerabilities described in CVE-2019-13450 and CVE-2019-13567, as well as new vulnerabilities described here:

- CVE-2020-11469
- CVE-2020-11470
- CVE-2020-11500

Policies you create with these templates detect Windows and macOS™/OS X® endpoints that run *vulnerable or outdated versions of Zoom*. Managed endpoints are evaluated. Endpoints are sorted into Forescout groups according to their level of vulnerability and detected software version. Apply further tests or appropriate remediation actions to each group.

Requirements

- The Forescout Endpoint Module *OS X Plugin* must be running

Limitations

Under certain conditions the Zoom application is falsely reported as potentially vulnerable, as a result of an inaccurate identification of the Zoom applications version number.