

Version Information: Security Policy Templates version 20.0.3

What's New?

This section describes the templates provided in this release. In the Policy creation wizard, these templates are available under the *Vulnerability and Response* sub-folder in the *Templates* tree.

- New template: [VR SMB Ghost](#)
- [Fixed Issues](#)

VR SMB Ghost

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 [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.

Fixed Issues

This section describes fixed issues for this release.

Policy Template	Issue	Description
VR CDP	SPT-381	Potentially vulnerable Nexus routers were incorrectly detected as not vulnerable.

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, 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 details of working with Forescout policies, see the *Forescout Administration Guide*.

- 📄 *Review and understand the detection/logic model provided by Forescout in these templates before you add or edit rules, or make more extensive customizations.*

For details about individual policy templates, see the *Security Policy Templates Configuration Guide*.

Requirements for Security Policy Templates

In addition to the requirements in this section, see the requirements for each template you wish to implement.

General:

- Windows Vulnerability DB 18.0.1 or above. Windows Vulnerability DB 18.0.5 or above to work with the VR CredSSP template.
- Windows PowerShell scripts must be allowed to run on Windows managed endpoints running Windows 7, Windows 20XX Server or above for working with VR Foreshadow, VR Meltdown and VR Spectre templates.
- 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.
- To run policy actions on endpoints with Remote Inspection, the user must have administrator privileges.
- To create policies that classify the network into CounterACT groups, make sure that either a Primary Classification or an Asset Classification policy is running on relevant endpoints, and The Add to Group actions in the classification policy are enabled.
- To take advantage of more precise classification profiles, create and run Primary Classification policies instead of Asset Classification policies.

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](#).

If you are working with CounterACT 8.0, Forescout 8.1, or Forescout 8.2:

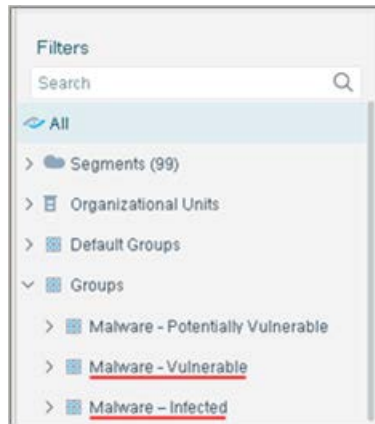
- Networking Module version 1.0 with the following components running:
 - Wireless Plugin for working with VR WPA2 KRACK and VR Cisco IOS/IOS-XE security templates.
 - VPN Concentrator for working with VR ASA security templates.
 - Switch Plugin for working with VR Cisco IOS/IOS-XE or VR CDP security templates.
- Endpoint Module version 1.0 with the following components running:
 - Linux Plugin for working with VR Intel SA-00075 AMT/ISM/SBT, VR Intel SA-00086 ME/SPS/TXE, and VR AMDflaws security templates.
 - OS X Plugin for working with VR macOS High Sierra Admin Bypass and VR AMDflaws security templates.
- Core Extensions Module version 1.0 with the Advanced Tools Plugin installed and running.

If you are working with CounterACT 7.0.0:

- An active Maintenance Contract for CounterACT devices is required.
- Wireless Plugin 1.5.1 or above must be installed and running to work with VR Cisco IOS/IOS-XE security templates.
- Switch Plugin 8.7.3 or above must be installed and running to work with VR Cisco IOS/IOS-XE or VR CDP security templates.
- Wireless Plugin 1.7.0.2009 or above is required for working with VR WPA2 KRACK security templates.
- VPN Concentrator Plugin 4.0.6 or above installed and running for working with VR ASA security templates.
- Linux Plugin version 1.1.0 or above installed and running for working with VR Intel SA-00075 AMT/ISM/SBT, VR Intel SA-00086 ME/SPS/TXE, and VR AMDflaws security templates.
- OS X Plugin version 1.2.0 or above installed and running for working with VR macOS High Sierra Admin Bypass and VR AMDflaws security templates.
- Advanced Tools Plugin version 2.2.0.1 or above installed and running.

Tracking Vulnerable and Infected Endpoints

To let you track infected and vulnerable endpoints for further handling, policies assign endpoints to Forescout groups based on policy evaluation. The plugin creates the Malware-Vulnerable and Malware-Infected groups and parallel Inventory views. In addition, specific policies may create other groups.




Known Issues

This section describes known issues for this release.

Issue	Description
SPT-107	AMD has not provided a patch for the vulnerabilities at this time. However, since the detection for the vulnerability is done by CPU type, the vulnerability will be reported as a false positive once the patch is available and has been applied.
SPT-119	Some Vulnerability and Response policies have a high CPU consumption when activated. CounterACT users should take this into account.
SPT-127	The Wireless plugin does not report IOS version for Cisco Wireless Controllers (WLC). As a result, WLCs are not detected as vulnerable by the VR Cisco IOS/IOS-XE. Workaround: WLC can be found vulnerable by checking the vulnerability state of Lightweight Access Points.
SPT-377	If you are working with CounterACT 7.0.0 service pack 3.0.2.5 , CounterACT 8.0.1.2 , or Forescout 8.1.2.3 , the following policy templates are not deployable: VR Cisco RV, VR Citrix, VR Exim, VR GoAhead, VR IoT Reaper, VR Jira, VR Mirai, VR PHP, VR VPNFilter Malware. For more information and assistance, please contact Forescout Customer Care.

Installation

Before installing the latest Security Policy Templates, make sure you have installed all the required dependencies, for example, the Windows Vulnerability DB.

 *To benefit from the updated policy templates provided in this release, it is recommended to remove previously created policies from CounterACT and create and activate new policies based on this release.*


If you are working with CounterACT 8.0 or above:


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.*

If you are working with CounterACT 7.0.0:**To install the plugin:**

1. Navigate to the [Product Updates Portal, Base Plugins](#) page and download the plugin `.fpi` file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin `.fpi` file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

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 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.