ForeScout

Solution Brief

Addressing WannaCry and Other Vulnerabilities with ForeScout Security Policy Templates

Use visibility, control and orchestration to reduce your attack surface and unify response

Ransomware is a particularly obnoxious form of malware. Experts strongly recommend against paying ransoms. Doing so won't make your other losses go away—and in most instances, payment won't result in unlocking your data. Fortunately, ForeScout can help you avoid ransomware through proper cyber hygiene and quickly detect, evaluate and respond to vulnerabilities and threats if required.

The Challenge

Vulnerability Assessment is considered a security best practice and is an important part of any security program. The notorious WannaCry and Petya ransomware campaigns targeted hundreds of thousands of users across multiple industries in close to 150 countries and caused disruption to organizations and critical infrastructure around the globe. Petya is similar to WannaCry in that it impacts Windows systems, and a successful infection results in encrypting the contents of the hard disk. However, unlike "traditional" ransomware attacks, Petya attacks appear to encrypt files without the ability to decrypt them later. Therefore, successful attacks may result in effectively wiping the encrypted files, with backups being the only definitive data recovery method. Once the initial system is infected, propagation methods include the ETERNALBLUE exploit that targets a vulnerability in the SMBv1 protocol (Microsoft Security Bulletin MS17-010), which was also used in the WannaCry ransomware attacks.

Addressing Ransomware like WannaCry and Petya

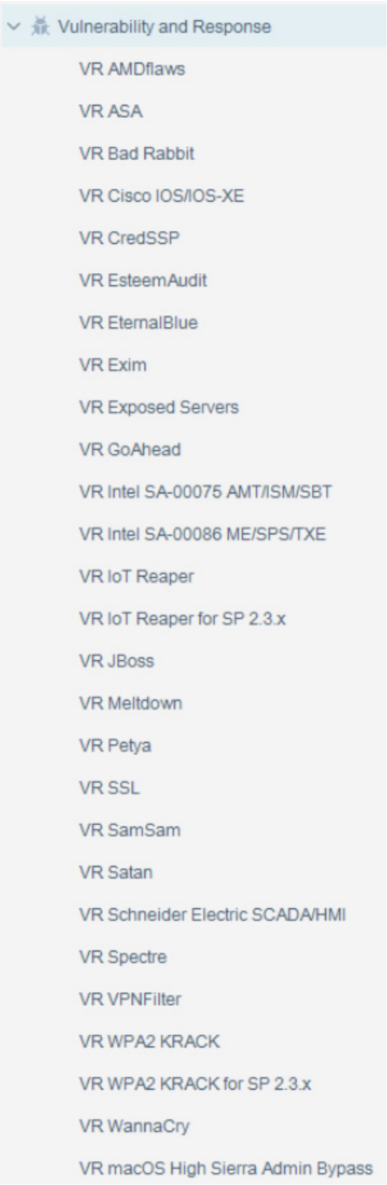
Microsoft published patches to resolve the SMB vulnerability for supported Windows versions on March 14, 2017 (Microsoft Security Bulletin MS17-010). The ForeScout publication, HPS vulnerability DB 17.0.3, released on March 20, 2017, includes this vulnerability update.

ForeScout has developed security policy templates that help to quickly identify and mitigate WannaCry ransomware attacks and other malware by facilitating the rapid response to an outbreak with an automated policy that quickly locates vulnerable hosts and determines which require patches and which are infected.

ForeScout Orchestration Advantages

The combination of ForeScout Extended Modules and the ForeScout platform enables sharing of contextual device data between ForeScout and other IT and security products. For example, the ForeScout platform can:

- Inform an endpoint protection platform to install/repair missing or broken agents and offer capabilities to assist in remediation.
- When the exact makeup of the ransomware is not known, as is typically the case with zero-day exploits, the ForeScout platform can leverage bi-directional information sharing with advanced threat detection and vulnerability assessment systems to automate policy-based security actions in real time.
- Block communication to a ransomware's command and control server if the indicator of compromise is known, as well as receive updates from popular advanced threat detection products and use them to block data exfiltration and collect the information.
- Initiate on-demand vulnerability assessment (VA) scans, identify the vulnerabilities exploited by ransomware and work with your VA systems to address them.
- Alert SecOps staff about security threats and risk levels with information obtained from a security information and event management (SIEM) platform. If needed, the ForeScout platform can also take response mitigation actions on devices based on correlations and feeds coming into the SIEM system.



Vulnerability and Response

- VR AMDflaws
- VR ASA
- VR Bad Rabbit
- VR Cisco IOS/IOS-XE
- VR CredSSP
- VR EsteemAudit
- VR EternalBlue
- VR Exim
- VR Exposed Servers
- VR GoAhead
- VR Intel SA-00075 AMT/ISM/SBT
- VR Intel SA-00086 ME/SPS/TXE
- VR IoT Reaper
- VR IoT Reaper for SP 2.3.x
- VR JBoss
- VR Meltdown
- VR Petya
- VR SSL
- VR SamSam
- VR Satan
- VR Schneider Electric SCADA/HMI
- VR Spectre
- VR VPNFilter
- VR WPA2 KRACK
- VR WPA2 KRACK for SP 2.3.x
- VR WannaCry
- VR macOS High Sierra Admin Bypass

Here is a sample of current ForeScout vulnerability response templates.

The security policy templates include the ability to identify:

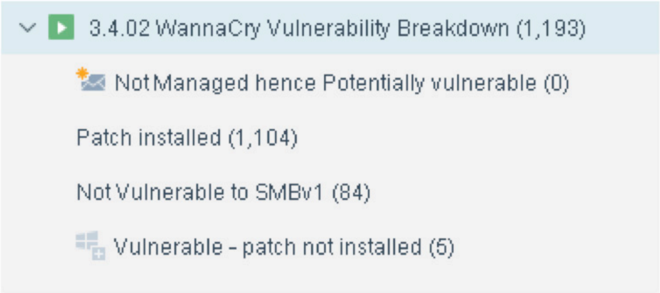
- WannaCry-vulnerable endpoints
- WannaCry-infected endpoints
- Petya-infected endpoints
- Petya-vaccinated endpoints

Organizations can quickly create policies using these templates and add actions to mitigate the risks related to vulnerable and infected endpoints. These templates also include support for Windows versions that are no longer officially supported by Microsoft: Windows XP, Windows 8 and Windows Server 2003. ForeScout can update the endpoints running these OSes with the appropriate patch by using native Windows domain policies or by leveraging third-party EPP agents from McAfee®, FireEye® and Symantec®. If needed, ForeScout can also help block ports that are vulnerable (TCP 445 used for SMB, ports 137-139 used for NetBIOS) for all boundary devices. ForeScout can also work with third-party systems to update antivirus applications and keep them up to date. As an additional layer of security, vulnerable endpoints, especially ones running older Windows versions, can be placed on restricted network segments, limiting access.

Addressing WannaCry and Other High-Profile Vulnerabilities with ForeScout

ForeScout's Cyber Event Response Team (CERT) monitors global security threats and assesses the potential vulnerabilities and impact to ForeScout customers. The team regularly releases Security Policy Templates to address these threats. Security Policy Templates are pre-built policy templates that use existing ForeScout functionality to detect, evaluate and respond to vulnerabilities and threats. Policies derived from these templates can provide customers with instant visibility, options for a fast and simple response, and the ability to track and segment devices that cannot be patched or mitigated.

Example: ForeScout Security Policy Template for WannaCry:



3.4.02 WannaCry Vulnerability Breakdown (1,193)

- Not Managed hence Potentially vulnerable (0)
- Patch installed (1,104)
- Not Vulnerable to SMBv1 (84)
- Vulnerable - patch not installed (5)

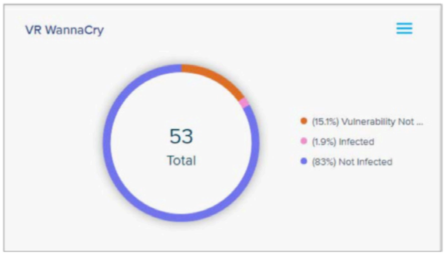
The screenshot above is an example of the WannaCry Security Policy Template. Devices are checked based on various criteria and information that ForeScout already knows about the device, including registry settings, patches applied and missing, Windows services running, operating system version and many other attributes.

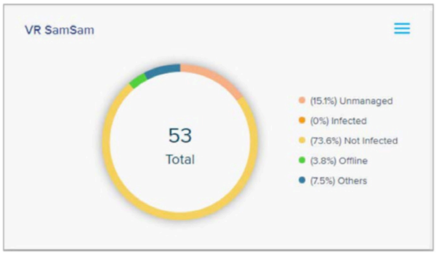
In the example above, devices that are determined to be vulnerable to WannaCry are automatically patched. ForeScout offers a wide range of other automated actions including notification actions (via email, Syslog to SIEM, etc.), host-based actions (run a script to disable SMBv1, etc.), and network-based actions (isolate the device, restrict the device with an ACL or VLAN, etc.).

> “ForeScout provided actionable visibility into the posture of every device on our network. The nuanced, actionable remediation options ForeScout offers allowed us to take a surgical approach to reducing risk and vulnerability of our network.”
>
> **— Yaron Levi, CISO at Blue Cross Blue Shield of Kansas City**

Security Policy Reports in the ForeScout Dashboard

Beginning with version 18.0.7, the ForeScout Dashboard (CounterACT 8.0) automatically creates a new widget for each installed Security Policy Template. The widget reports the current discovery status of the policy. Below you see the VR WannaCry and VR SamSam Security Policy Template Dashboard widgets:





Other Vulnerabilities Addressed by ForeScout Security Policy Templates.

In addition to WannaCry, Petya and SamSam, ForeScout provides Security Policy Templates designed to help customers accurately identify vulnerable systems and respond to high-profile vulnerabilities (see sidebar on page two), including those affecting IT infrastructure devices such as switches, routers and Internet of Things (IoT) devices. These regularly updated and released example policies can be implemented by customers to continuously monitor their environment and take automated actions when vulnerabilities are discovered.

Learn more

Experience the before-and-after difference of the ForeScout platform with a hands-on Test Drive that takes you through powerful solutions, including how to respond to a WannaCry outbreak by using an automated policy.
Visit www.forescout.com

Learn more at
www.ForeScout.com

ForeScout®

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591