# Security Policy Templates 20.0.13 Release Notes

## Templates Provided or Modified in This Release

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

- VR SolarWinds Orion
- VR AMNESIA:33 (Update)

🗎 *The database is cumulative: this release includes all previous* Vulnerability and Response *templates and updates.*

### 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*

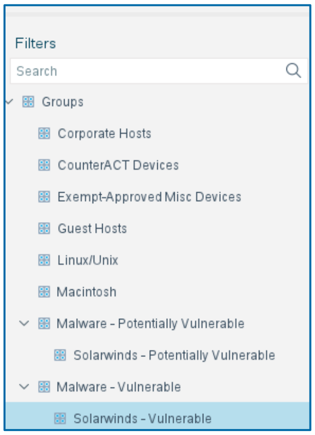
Endpoint vulnerability is determined based on the presence of SUNBURST malware and other suspicious SolarWinds applications and services, related open ports, and other factors.

🗎 *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.*

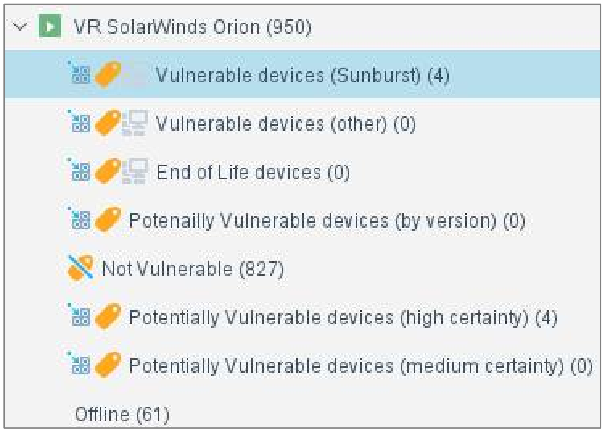
*As information about this exploit develops, or the attack adapts, modify your policies to search for other application drop/installation locations.*

### ***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.



Filters
Search
Groups
Corporate Hosts
CounterACT Devices
Exempt-Approved Misc Devices
Guest Hosts
Linux/Unix
Macintosh
Malware - Potentially Vulnerable
Solarwinds - Potentially Vulnerable
Malware - Vulnerable
Solarwinds - Vulnerable



VR SolarWinds Orion (950)
Vulnerable devices (Sunburst) (4)
Vulnerable devices (other) (0)
End of Life devices (0)
Potenailly Vulnerable devices (by version) (0)
Not Vulnerable (827)
Potentially Vulnerable devices (high certainty) (4)
Potentially Vulnerable devices (medium certainty) (0)
Offline (61)

- 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.<br>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 AMNESIA:33 (Update)

This release provides updates to the AMNESIA:33 policy template that was recently released in version 20.0.12. This update adds additional inspection scripts and detection conditions that focus on vulnerable instances of the Nut/Net TCP/IP stack.

### *About AMNESIA:33*

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

- uIP
- FNET
- picoTCP
- Nut/Net

***Four of the vulnerabilities received a critical CVSS 3.x Severity Rating score, and allow Remote Code Execution.*** *They could allow an attacker to steal data, overload systems (Denial of Service attack) or even take control of the devices.*

***These vulnerabilities reside inside millions of devices*** *due to the open source nature of the stacks and their prevalence. The stacks affected by AMNESIA:33 are found in embedded devices, systems-on-a-chip, networking equipment, OT devices, and a myriad of consumer and enterprise IoT devices.*

Policies created with this template use passive and active techniques for full visibility into potentially vulnerable devices across all parts of the network. In sensitive environments, such as OT and medical IoT, only passive techniques can be used.

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

This template is compatible with CounterACT 8.0.x and above. If you are running CounterACT 8.0.x or 8.1.x you may need to upgrade to a supported Hotfix. See the *Security Policy Templates Configuration Guide* for details.

## 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.<br>Workaround: WLC can be found vulnerable by checking the vulnerability state of Lightweight Access Points. |
| **SPT-377** | Policy templates that use encrypted parameters cannot be deployed on some supported Forescout releases. Affected policy templates currently include Cisco RV, VR Citrix, VR Exim, VR GoAhead, VR IoT Reaper, VR Jira, VR Mirai, VR PHP, VR VPNFilter Malware, and VR AMNESIA:33. Upgrade to the following releases to resolve this issue:<br>▪ 7.0.0 Hotfix 3.0.2.5 and above<br>▪ 8.0.1.2 and above<br>▪ 8.1.2.3 and above<br>▪ 8.1.3.1 and above<br>▪ 8.2.x and above |
| **ADT-279**<br>**ADT-292** | If you are working with Forescout 8.2.1, *CounterACT Script Result* conditions that generate traffic might fail. Affected policy templates currently include VR Ripple20, VR Ripple20 Vulnerability Scanner, and VR AMNESIA:33. To resolve this issue, upgrade to the latest Advanced Tools Plugin 2.4.1 hotfix. For assistance, contact your support representative. |

## Install the Module

This section describes how to install the 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.*

## More Information

For more information on how to work with Security Policy Templates and Security Policy Templates Module Requirements refer to the *Security Policy Templates Configuration Guide*.

## 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 11:31