

ForeScout CounterACT®

Windows Vulnerability DB

Configuration Guide

Updated February 2018



Table of Contents

About the Windows Vulnerability DB Module	3
Module Requirements	. 3
Supported Windows Operating Systems and Other Products	.4
Distributing Vulnerability Information to Windows Endpoints	4
Minimize Bandwidth During Vulnerability File Download	.5
Using Vulnerability Information to Manage Endpoints	5
Vulnerability Reporting	6
About Installation	6
Configuration	. 7
Changes that Impact Windows Endpoints	.7
Additional CounterACT Documentation	7
Documentation Downloads	.7
Documentation Portal	.8
Counteract Help Tools	.8

About the Windows Vulnerability DB Module

The Windows Vulnerability DB is a Content Module that delivers vulnerability updates to CounterACT soon after they are released from Microsoft. These updates are used when working with vulnerability policies.

The HPS Inspection Engine, installed on each Appliance, instructs endpoints to download the information from the Windows Vulnerability DB when the **Microsoft Vulnerabilities** or the **Microsoft Vulnerabilities fine-tuned** property is used. SecureConnector is not required to download or work with Windows Vulnerability DB information on endpoints.

rulner	Microsoft Vuln	t <mark>erabil</mark> host	ities. Indicates the existence of Mid	crosoft pul	lished O	5 and Offi	se vulnera	bilities
 Properties Workfee Vulnerability Manager MvM Connection is UP MvM Scan Results 	Use of this property requires the proper configuration and activation of the HPS inspection Engine plugin.							plugin.
MVM Scan Status	Search		Q					
MVM Applied Tags	Na Cat	legery	Description	Updat	Sever	Rebo	More	CVE
✓ ♥ Windows Security	2017-0 Win	dows	A security issue has been identifi	2017-0	Critical	Can R	http://s	
Windows Update Agent Installed	2017-0. Win	dows	A security issue has been identifi.	2017-0	Critical	Can R	http://s	
Microsoft Vulnerabilities	2017-0Win	dows	A security issue has been identifi.	2017-0	Critical	Can B	http://s	
Microsoft Vulnerabilities Fine-tuned	2017-0 Win	dows	A security issue has been identifi.	2017-0	Critical	Can R	http://s	
	2017-0 Win 19 items (1 s	dows elected	A security issue has been identifi	2017-0	Critical	Pan R	intervise	
	Evaluate im	esolvat	ile criteria as 🛛 False 🗸			Add	Detail	s <u>C</u> lear

Vulnerability detections appear in the Console Details pane when you select the policy used to detect vulnerabilities.

> 🖿 HWI	redminote4-r	redmi.d	10.34.1.53	Win_ENV34	msv-all-policy	b0e235tce190	
> Ba Mac_Linux	DOM36IWIN	8	10.36.2.84	vuln	msv-all-policy	6254000072ab	10.36.1.250.15
- 🖿 MSV	DOM34IWIN	10-PRO	10.34.3.66	Win_ENV34	msv-all-policy	0050569f74ab	
> 🛄 External Disk Drive C	 DOM34\QA-I 	MINS	10.34.3.70	Win_ENV34	msv-all-policy	005056910a72	
msv fine tuned (7)	 DOM34VQ34 	WINS20	10.34.3.54	Win_ENV34	msv-all-policy	00505691715e	
msv-08 (0)	 DOM34VQ34 	WIN815	10.34.1.121	Win_ENV34	E msv-all-policy	005056b6fe42	
MSV-09 (5)	 DOM34\Q34 	WIN201	10.34.1.74	Win_ENV34	msv-all-policy	00505656491e	
msv-all-policy (9)	 DOM34\Q34 	WIN201	10.34.1.84	Win_ENV34	msv-all-policy		
Microsoft (0)	• DOM34VQ34	WIN10P	10 34 3.64	Win ENV34	msy-all-policy	0050669f6628	
MSV_Critical (7)	msv-all-policy	Profile	Compliance	All Policies			
MSV fine tune (9)							
Filters		MAC Ac	dministrator IPv4 ddress: 5254000	Address: 10.36 072ab Domain:	2.84 Hostname: WIN8 DOM36		
Search Q	March and Provide and Provide American Science and Provide American Scienc						
🗢 All	Matched the	ain Rule	ticy policy on Ocide	er 15 01;40:31 PM			
 Segments (234) 	Condition F	Properties	Microsoft Vulnerab	lities.	April 2017 Security Only	Update for NET Framework 3.5.4.5.2.4.6.4.6.1.4	4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KR4014987)
For classification (234)					May, 2017 Security Only 2017 20 Security Only 2	Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4	.8.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB4019111)
💦 Linux (1)					2017-09 Security Update	for Adobe Flash Player for Windows 8.1 for x64-ba	ased Systems (KB4038806)
🔐 Mobile (1)					2017-09 Security and Qu	ate for Internet Explorer 11 for Windows 8.1 for x64 ality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6	I-based Systems (KB4040685) I.1, 4.6.2, 4.7 on Windows 8.1 and Server 2012 R2 for x64 (KB4041085)
💕 OSX (3)					2017-09 Security Only U 2017-10 Security Only Q	idate for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6 ality Update for Windows 8.1 for x64-based Syste	(2, 4,7 on Windows 8.1 and Server 2012 R2 for x84 (KB4041092) ms (KB4041687)
3 Sim_seg (0)					2017-10 Security Monthl	Quality Rollup for Windows 8.1 for x64-based System for Microsoft Visual C++ 2010 Service Red 1	Mems (KB4041693)
> 💣 Stas-Windows (6)					MS15-041 Security Upo	ate for Microsoft .NET Framework 3.5 on Windows	8.1 and Windows Server 2012 R2 for x64-based Systems (KB3037576)
😽 vuin (1)	Actions:		None (No actions o	sefined for this rule	0		
🗸 💏 Windows (15)	Sub-Rules:						
> di Win ENV34 (14)							

Module Requirements

The module requires CounterACT version 8.0.

Supported Windows Operating Systems and Other Products

The following Windows operating systems are supported on 32-bit and 64-bit machines.

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

In addition, network server and productivity packages that are updated through the Windows Updates facility are supported.

Distributing Vulnerability Information to Windows Endpoints

There may be situations when it is more efficient for endpoints to retrieve vulnerability information from WSUS or Windows Updates, rather than use the information provided by the Windows Vulnerability DB.

It is recommended to continue using WSUS or Windows Update in the following situations:

- When a local WSUS instance is deployed in your network environment.
- When endpoints are connected to your network through a VPN and are physically located at a distance from the Appliance, it may be faster for the endpoint to retrieve vulnerability information directly from the Microsoft Updates website or a local WSUS.

When they are available, you may use other methods to distribute the Microsoft Vulnerability CAB file to endpoints in your environment.

The HPS Inspection Engine looks for the following file on Windows endpoints:

%systemroot%\temp\wsusscn2.cab

If this file is different than the CAB file provided by the Windows Vulnerability DB, CounterACT downloads its own CAB file to the endpoint.

Refer to the HPS Inspection Engine Configuration Guide *for details of configuration to use WSUS or Windows Updates.*

Minimize Bandwidth During Vulnerability File Download

You can minimize bandwidth usage during Microsoft vulnerability file download processes by limiting the number of concurrent HTTP downloads to endpoints. The default is 20 endpoints simultaneously.

To customize:

- 1. Select Tools>Options>HPS Inspection Engine>Windows Updates tab.
- 2. Define a value in the Maximum Concurrent Vulnerability DB File HTTP Uploads field.

Remote Inspection	SecureConnector	Windows U	pdates	Classification	Tuning	Test				
Use endpoint's "Windows Updates" settings (WSUS, MS Website) to check for missing updates										
From		Т	`о				<u>A</u> dd			
10000		10	0.0.0.255				<u>E</u> dit			
							<u>R</u> emove			
1 items (0 selected)										
WSUS Environment	Settings									
HTTP(S) URL of WSU	5 server									
HTTP(S) URL of repor	tserver									
Windows Update De	fault Settings									
Update method			Automati	ally Download a	nd Notify of Ir	istallation \checkmark				
Maximum Concurrent	Vulnerability DB File H	TTP Uploads	40							

Using Vulnerability Information to Manage Endpoints

This section describes recommended best practices for detecting and remediating vulnerabilities on endpoints.

To work with vulnerability information:

- 1. Create a policy based on the Windows Updates Compliance policy template. This policy uses the Microsoft Vulnerabilities property to check Windows endpoints for vulnerabilities related to all Knowledge Base issues downloaded from Microsoft.
 - By default, the Check new vulnerabilities automatically option is enabled, so that the policy automatically checks for new vulnerabilities added when the Windows Vulnerability DB is updated.
 - The policy provides the Start Windows Update action to update endpoints that are missing patches for known vulnerabilities. By default, this action is disabled. It is recommended to enable this action.
- 2. Accept default scheduling/recheck behavior for the policy.

For more details, and for information on remediating vulnerabilities on Linux and MacOS/OS X endpoints, see the <u>Control Network Vulnerabilities How-to Guide</u>.

Vulnerability Reporting

You can also generate reports that display the vulnerability status of selected Windows hosts. The report displays the number and percentage of hosts with vulnerabilities versus those that have no vulnerabilities, and lists the relevant hosts.

To create a report based on vulnerability information:

- 1. Select Reports by clicking on the ellipsis icon from the CounterACT toolbar.
- 2. The Reports portal opens.
- 3. Select Add. The Add Report template Wizard opens.
- 4. Select the Vulnerability Report template.

		Report Templates	Description	1
0	1	Assets Inventory	Show an inventory of selected assets.	
⊙	1	Vulnerability	Show the vulnerability status of selected Windows hosts.	
o	hall	Policy Trend	Show policy results over a selected period of time.	
o		Policy Status	Show the policy status for selected hosts.	
0	14	Policy Details	Show detailed results for a selected policy.	
0	1	Compliance Status	Show the compliance status of selected hosts.	
0		Device Details	Show detailed information of selected devices.	
0	1	Registered Guests Analysis	Show guest registration inventory information.	
0	m	Registered Guests	Show guest device information.	

5. Follow the wizard instructions to create the report.

Vulnerability Report	ForeScout
Report Deatils	
Hosts: 'All IP's'	
Generated By: Administrator	
Generated At: Wed Jul 09 14:28:55 IDT 2008	
Description: Vulnerability Report	
Vulnerable Hosts Summary	
Vulnerabl	Hosts Summary
Uunerable Ho	ts 🔲 Non Vulnerable Hosts
7/9/06 2:28 PM	Page 1 of 2

About Installation

After installation of the Windows Vulnerability DB Module, the HPS Inspection Engine is restarted.

Configuration

Sources and settings for Windows Updates are configured in the HPS Inspection Engine. For example, see <u>Minimize Bandwidth During Vulnerability File Download</u>. For more information about Windows Updates settings, see the *HPS Inspection Engine Configuration Guide*.

Changes that Impact Windows Endpoints

The plugin installs the following file(s) on endpoints.

Name	Description
fs_wua_search.vbs	Resolves Microsoft Vulnerabilities properties.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- <u>Documentation Downloads</u>
- <u>Documentation Portal</u>
- <u>CounterACT Help Tools</u>

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- Per-Appliance Licensing Mode Product Updates Portal
- Centralized Licensing Mode <u>Customer Portal</u>
- Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see <u>Identifying Your</u> <u>Licensing Mode in the Console</u>.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- 1. Go to https://updates.forescout.com/support/index.php?url=counteract.
- 2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

- 1. Go to https://forescout.force.com/support/.
- 2. Select Downloads or Documentation.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

- 1. Go to <u>www.forescout.com/docportal</u>.
- 2. Use your customer support credentials to log in.
- 3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select CounterACT Help from the Help menu.

Plugin Help Files

- 1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
- 2. Select the plugin and then select Help.

Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options** > **Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Options			
Search Q	Licenses Activate, update or deactivate your licen	se for CounterACT features and Extend	ded Module
© Discovery	Search	Q Status	Туре
ticenses	ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
Tists	ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
> 🕊 Map	ForeScout CounterACT Resiliency ForeScout Extended Module for Check	Valid Point Next Valid, Capacity exceeded	Perpetual Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <u>https://www.forescout.com/company/legal/intellectual-property-patents-trademarks</u>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-10 09:21