Flexera

Software Vulnerability Manager 2019 (Cloud Edition) Release Notes

December 2019

Introduction1	L
New Features and Enhancements 2	
Vendor Patch Module - Automation	2
Software Vulnerability Manager Client ToolKit4	
Flexera SVM Patch Configuration4	4
Flexera WSUS Management Tool6 Extended Support in Non IE Browser	6
Extended Support in Non IE Browser	B
CVE Number as Criteria in Host Smart Groups9	9
Resolved Issues	Э
Product Feedback	C
System Requirements)
Legal Information	L

Introduction

Flexera's Software Vulnerability Manager 2019 is a Vulnerability and Patch Management Software Solution that facilitates a customized Patch Management process. It combines Vulnerability Intelligence, Threat Intelligence, Vulnerability Scanning, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.

Vulnerability and Patch Management are critical components of any security infrastructure because they enable proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With Software Vulnerability Manager 2019, IT Operations and Security Teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, Mac OS, and Red Hat Enterprise Linux.

Software Vulnerability Manager 2019 integrates seamlessly with Microsoft[®] WSUS and System Center Configuration Manager.

New Features and Enhancements

Software Vulnerability Manager 2019 (Cloud Edition) includes the following new features and enhancements:

- Vendor Patch Module Automation
- Software Vulnerability Manager Client ToolKit
- Extended Support in Non IE Browser
- CVE Number as Criteria in Host Smart Groups

Note • To see the following new features and enhancements in your Software Vulnerability Manager 2019 interface, you must refresh your browser's cache (press Ctrl+F5).

Vendor Patch Module - Automation

With this release of Software Vulnerability Manager 2019, users can automate deployment of patches supported by Vendor Patch Module. The new option **Subscribe to Package** has been added to right click menu. Subscribed packages will be deployed automatically to configured WSUS using a new tool called **Flexera SVM Patch Configuration**, see Software Vulnerability Manager Client ToolKit.

Note • Install Software Vulnerability Manager Client ToolKit to utilize the Vendor Patch Module - Automation.

To use this option, navigate to **Patching >> Vendor Patch Module**. List of patches appears, you can know a patch whether it is already subscribed and its status in the **Subscribed** and **Subscription Status** column.

Search Type: Product	Search text	Search V	lew from the c	ontext of S	mart Group:	Not Selected		✓ Configure Vie	ew		
Product 🔺	Vendor	Patched Version	Deploym	SAID	Criticality	Threat Sc	Advisory Publish	Architecture	Insecu	Subscribed	Subscription Started
1Password	AgileBits	7.3.712.0	Yes	-	-	-	-	Windows 32-bit	(Yes	8th Dec, 2019 17:0
4K Video Downloader	OpenMedia	4.10.1.3240	Yes	-	÷		÷	Windows 64-bit	0	Yes	8th Dec, 2019 17:0
4K Video Downloader	for Mac OpenMedia	4.10.0.3230	No	-	÷	-	-	Mac Intel 64-bit	0	No	
5KPlayer (x64)	DearMob Inc.	6.1.0.0	No	-	-	-	-	Windows 64-bit	0	No	
5KPlayer (x86)	DearMob Inc.	6.1.0.0	No	-	÷	-	-	Windows 32-bit	0	No	
5KPlayer for Mac	DearMob Inc.	6.1.0.0	No	-	-	-	-	Mac Intel 64-bit	0	No	
7-Zip (x64)	Laor Davlov	19.00.00.0	Yes	-	-	-	-	Windows 64-bit	1	No	
7-Zip (x86)	Create Update Package	19.00.00.0	Yes	-	-	-	-	Windows 32-bit	(No	
ABBYY FineRead	View Installations	15.0.1496.0	No	-	-	-	-	Windows 64-bit	0	No	
ABBYY FineRead	Patch Information	15.0.1496.0	No	-	-	-	-	Windows 32-bit	0	No	
Accumulated ho	h	21.0.52.0.4	No	<u>SA908</u>		-	27th Aug, 2019	Windows 64-bit	0	No	
Accumulated ho	Subscribe to Package	20.1.107.0.19	No	<u>SA908</u>		-	27th Aug, 2019	Windows 64-bit	0	No	
Accumulated hotfix 1	for Au Autodesk Inc.	21.0.52.0.4	No	<u>SA908</u>		-	27th Aug, 2019	Windows 32-bit	0	No	
Accumulated hotfix 1	for Au Autodesk Inc.	20.1.107.0.19	No	<u>SA908</u>		-	27th Aug, 2019	Windows 32-bit	0	No	
ACDSee (32-bit)	ACD systems Internati	20.4.0.630	Yes	-	-	-	-	Windows 32-bit	0	Yes	20th Nov, 2019 15:2
ACDSee (64-bit)	ACD systems Internati	20.4.0.630	No	-	-		-	Windows 64-bit	0	No	
Acrobat 10.1.16 Pro a	ind St Adobe	10.1.16.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	0	No No	
Acrobat 11.0.23 Pro a	ind St Adobe	11.0.23.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	0	No	
Acrobat DC Pro and S	tanda Adobe	17.11.30152.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	0	NO NO	
Acrobat DC Pro and S	tanda Adobe	15.006.30505.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	0	NO	
Acrobat DC Pro and S	tanda Adobe	19.021.20056.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	3	No	
Acrobat Reader 2017	Classi Adobe	17.008.30051.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	0	NO NO	
Acrobat Reader 2017	Classi Adobe	17.11.30152.0	No	<u>SA890</u>		12	15th Oct, 2019	Windows 32-bit	0	No	
ActivDriver x64	Promethean Ltd	5.16.7.0	No	-	-	-	-	Windows 64-bit	0	No	
ActivDriver x86	Promethean Ltd	5.16.7.0	No		-	-	-	Windows 32-bit	0	No	
•	1 of 55 🕨 🕅 🚑										

Right click on a patch which you want to subscribe, select the option Subscribe to Package.

Configure Subscription dialog pane appears, you can choose your preferences from the below options:

Configure Subscription - Firefox (English US) (:	x64)		×					
Always publish a new patch when a new vers	ion is available							
Only publish a new patch when any of the following of	lowing are true:							
SAID CVSS3 score is greater than	0	¥						
Criticality is greater than	Not Critical	¥						
Threat score is greater than	0	¥						
Patched version greater than	71.0.0.0							
 Trigger subscription rule above now for the construction rule above next time a number of the construction rule above next time a num								
Package configuration Use Flexera custom naming								
		Save Cancel						

Either one of the below preferences must be defined:

- Always publish a new patch when a new version is available Publishes when new version of the patch is available.
- Only publish a new patch when any of the following are true: Publishes when any one of the defined preferences are met. To know more about the below preferences, see Appendix B About Secunia Advisories.
 - SAID CVSS3 score is greater than
 - Criticality is greater than
 - Extremely Critical
 - Highly Critical
 - Moderately Critical
 - Less Critical
 - Not Critical
 - Threat score is greater than
 - Patched version greater than By default, current version of a patch will be displayed.

Either one of these option must be selected to define the deployment schedule based on above preferences:

- Trigger subscription rule above now for the current version Publishes the package right away.
- **Trigger subscription rule above next time a new version is available** Start publishes the package when newer version is available.

Software Vulnerability Manager Client ToolKit

In addition to the SVM Multi-Partition Reporting Tool introduced earlier this year, to ease patch automation and WSUS management two tools have been newly added to the **Software Vulnerability Manager Client ToolKit**.

On successful installation of **Software Vulnerability Manager Client ToolKit**, below tools will get install and their respective shortcuts will be created in your desktop.

- Flexera SVM Patch Configuration
- Flexera WSUS Management Tool

Prerequisites

The below prerequisites are required:

- .Net Framework 4.6.1 and above.
- OS Requirements:
 - Install Software Vulnerability Manager Client ToolKit in Windows Server 2012 or Windows 8, for Windows 2012 WSUS.
 - Install Software Vulnerability Manager Client ToolKit in Windows Server 2016 or Windows 10, for Windows 2016 WSUS.
- Install both the Software Vulnerability Manager Patch Configuration and WSUS in the same domain.



Important • You must install *Software Vulnerability Manager Patch Client ToolKit* to utilize the Vendor Patch Module - Automation. To download this ToolKit, click here.

Flexera SVM Patch Configuration

Flexera SVM Patch Configuration integrates Software Vulnerability Manager application with the configured WSUS server to achieve the automation for subscribed packages.

Flexera SVM Patch Configuration, has three tabs:

- WSUS Connection
- SVM Connection
- General

WSUS Connection

WSUS Connection tab prompts you to enter WSUS server credentials and helps you to select computer groups which you want to deploy the packages.

Flexera SVM Patch Confi	guration	- 🗆 🗙
WSUS Connection SVM Connection General	Output Window:	Clear Output
Server: Pot: Use SSL Groups to auto deploy: All Computers Unassigned Computers Win7 Computers	a. J. And Section 1997 Use served to a 28 42 AMI (EMICAL Under to come Provide the Comparison of the Comparison of the Provide the Comparison of the Comparison of the Comparison according to commend to according to the Comparison of the A 28 53 AMI (Second A) commended to process according 1997 According a 28 53 AMI (Second A) commended a 28 53 AMI (Second A) commended a 28 53 AMI (Second A) (Second A) a (Second A) (Second A) (Second A) a (Second A) (Second A) (Second A) a (Second A) (Second A) (Second A) (Second A) (Second A) a (Second A) (Second A) (Second A) (Second A) (Second A) a (Second A) (Second A) (Second A) (Second A) (Second A) a (Second A) (Second	work of to WSUS An unexpected WSUS:
Win10 Win8 ✓	6.2553.488] Targeting/Rode: Server 9.2553.488] ProcyServerFet: 80 9.2553.488] Attempting to datase the progetime IN2525. 9.2553.488] Number of computer targ	orguðer læget ef gruges 1
Flexera SVM Patch will connect to the WSUS server under the running Windows user context.		
Load Groups		

SVM Connection

SVM Connection tab prompts you to enter a SVM credentials and token will be generated on successful connection.

Flexera SVM Patch Co	nfiguration – 🗆 🗙
WSUS Connection SVM Connection General	Output Window: Clear Output
Connect to On-Prem SVM Server Site URL: Use SSL	A 22 44 AM December 24 47 48 48 48 49 49 49 49 49 49 49 49 49 49 49 49 49
User Name: Password:	A State of a monotonic second se
Test Connection	I 4:37:18 AMJ Token: BH2dfaddVeldg1wMCwu47bjQ0() twOXClejdkpp9gW RJsB5RNOz1WBQBrwLP/WJ

General

In general tab, you can define the folder path for log files and log level need to be captured. You can set the frequencies to trigger the polling in Check-In Settings.

E Flexera SVM Patch Conf	iguration – 🗆 🗙
WSUS Connection SVM Connection General Logging	Output Window: Clear Output

Flexera WSUS Management Tool

Flexera WSUS Management Tool allows you to manage the packages and configuration settings of WSUS.

This Tool consist of below tabs:

- Patching Information
- Configuration

Patching Information

Patching Information tab prompts you to connect to the WSUS server to view the packages, based on the selected filter option, either 3rd party, Microsoft updates, or both. It also allows you to approve, delete, decline the selected patches and select a computer groups where you want to deploy these approved patches, at the set deadline.

It consist of three sections:

- Filter Update List
- Group Approvals
- Set Approval Deadline

MCUC C				-+ 0500						
NSUS <u>S</u> erv	er psccm.sccm.test		E	ort 8530		9.55L				
Patching Inf	formation Configuration									
Filter Upd	ate List	Group Appro	vals					_		
③ <u>3</u> rd Pa	arty	Compute					Set Approval Deadline			
	soft Updates		I Compute					12/ 9/2019		
O <u>A</u> I			_Unassi √win7	gned Com	puters			9:23:09 PM	÷	
Text Filter	r: Flexera		✓ win /					9:23:09 PM		
Connect	to Server and Refresh		win8			Approve Groups				
Number of	Updates Found: 30									
State	> Title	for Software Flexera for Software Flexera			Approval	Installed	Pending	Not Installed	^	
Ready	Deployment package for				Unknown	0	0	19		
Ready	Deployment package for			oftware	Unknown	0	0	18		
Ready	Deployment package for			oftware	Unknown	0	0	18		
Ready	Deployment package for			oftware	Unknown	0	0	18		
Ready	Deployment package for	Software	re Flexera Software		Unknown	0	0	18 17		
Ready	Deployment package for	Software			Unknown	0				
Ready	Deployment package for	Software			Unknown	0	0	17		
Ready	Update .NET Core Runtin	ne 3.1 (x	Mic	Dealing	Selected Updates		0	0		
Ready	Update 4K Video Downlo	ader, ver	Ope				0	6		
Ready	Update 7-Zip (x64), versio	on 19.00	Igor	Delete S	Selected Items		0	0		
Ready	Update 7-Zip (x64), versio	on 19.00	Igor	Export S	SDP file		0	0		
Ready	Update 7-Zip (x64), versio	on 19.00	Igor	Propert	iec		0	0		
Ready	Update 7-Zip (x64), versio	on 19.00	lgor	- Topen			0	0		
Ready	Update 7-Zip (x64), versio		Igor Pavl		Unknown	15	0	0		
Ready	Update 7-Zip (x64), versio	sion 19.00 Igor Pavl			Unknown	15	0	0		
Ready	Update 7-Zip (x64), versio		Igor Pavl		Unknown	15	0	0		
Ready	Update 7-Zip (x64), versio		Igor Pavl		Unknown	15	0	0		
Ready	Update 7-Zip (x64), versio		Igor Pavl		Unknown	15	0	0		
Ready				ov	Unknown	15	0	0	~	

Configuration

In Configuration tab, you can perform the below WSUS configuration actions:

- Test WSUS
- Test GPO Settings
- Generate New Signing Certificate
- Install Signing Certificate
- Export Signing Certificate from WSUS
- Delete Signing Certificate in WSUS
- Create / Update SVM Group Policy Settings
- Dump All GPO Informations

🚯 Win	dows Server Update Service Management Tool	_ 🗆 🗙
WSUS Server psccm.sccm.test	Port 8530 Use SSL	
Patching Information Configuration		
Operations to run:	Output Window:	Clear Output
Test WSUS Test GPO Settings		
WSUS Certificate Functions		
Generate New Signing Certificate		
Set External Signing Certificate		
Path: Browse		
Password:		
Set Signing Certifcate in WSUS		
Install Signing Certificate		
Export Signing Certificate from WSUS		
Delete Signing Certificate in WSUS		
Group Policy Functions		
GPO Name: WSUS - CSI		
GPO to Support SCCM Patch Deployment		
GPO to Install WSUS Certificate		
Create / Update SVM Group Policy Settings		
Dump All GPO Information		

Extended Support in Non IE Browser

In Software Vulnerability Manager 2019, list of products available in **Flexera Package System (SPS)** and **Patch Template** can also be seen in non IE browsers.

After successful login to the Software Vulnerability Manager 2019 in non IE browser (Chrome, Mozilla, etc.), Open **Patching**, below sections are now available in non IE browsers:

- Flexera Package System (SPS)
- Patch Template

	Flexera Package Syste	m (SPS)												
Deshboard	Search Type: Product	▼ Search text	Sea	rch View from	the context o	f Smart Group	All Products		✓ Configu	re View				Export +
	Product	Vendor +	Patched Version	Architecture	SAID	Criticality	Threat	Detected	Advisory P	Insecure	End-Of-Life	Secure	Total	Hosts
Scanning	7-zip		18.05	Windows64-bit	SA82839		2	5 months ago	1st May, 2018	1	3	0	4	4
~	7-zip 16.x		18.x	Windows32-bit	SA82839		2	8 months ago	1st May, 2018	0	1	0	1	1
Results	Calibre 2.x		3.x	Windows64-bit	SA81916		2	4 months ago	9th Mar, 2018	0	1	0	1	1
	FileZilla 3.x		3.43.0	Windows64-bit	SA89720			1 month ago	28th Jun, 2019	2	0	0	2	2
Reporting	FileZilla 3.x		3.43.0	Windows32-bit	SA89720			4 months ago	28th Jun, 2019	3	0	0	3	3
	Notepad++		7.7	Windows32-bit	SA91115		2	2 days ago	18th Sep, 2019	7	1	0	8	8
Patching	Notepad++ 7.x		7.7	Windows64-bit	SA91115		2	27 days ago	18th Sep, 2019	11	0	0	11	11
exera Package System (SPS)	TortoiseSVN 1.x		1.12.2	Windows64-bit	SA90536			27 days ago	14th Aug, 2019	3	0	0	3	2
Patch Template	UltraVNC 1.x		1.0.9.1	Windows64-bit	SA41208				30th Aug, 2010	2	0	0	2	1
endor Patch Module	WinSCP 5.x		5.15.5	Windows32-bi	SA91409			27 days ago	3rd Oct, 2019	20	0	0	20	19
	Adobe Acrobat Reader	Adobe Systems	2019.021.20047 (Windows32-bi	SA89000		12	2 days ago	15th Oct, 2019	5	10	0	15	15
Administration	Adobe Acrobat Reader	Adobe Systems	2015.006.30504 (Windows32-bi	<u>SA89000</u>		12	7 months ago	15th Oct, 2019	1	0	0	1	1
	Adobe Flash Player	Adobe Systems	32.0.0.255 (PPAPI)	Windows32-bi	SA90957		4	26 days ago	10th Sep, 2019	2	1	0	3	3
Configuration	Adobe Flash Player	Adobe Systems	32.0.0.255 (NPAPI)	Windows32-bi	SA90957		4	27 days ago	10th Sep, 2019	12	16	0	28	28
	Adobe Flash Player 9.x	Adobe Systems	32.x (ActiveX)	Windows32-bi	SA90957		4	51 days ago	10th Sep, 2019	0	3	0	3	3
	Apple iTunes 12.x	Apple	12.10.2	Windows64-bit	SA91817		-	27 days ago	31st Oct, 2019	3	0	0	3	3
	Apple (Tunes 12.x	Apple	12.10.2	Windows32-bit	SA91817			10 months ago	31st Oct, 2019	3	0	0	3	3
	Google Chrome	Google	78.x	Windows64-bit	SA92273		3	26 days ago	19th Nov, 2019	0	3	0	3	3
	Google Chrome	Google	78.0.3904.108	Windows32-bit	SA92273		3	27 days ago	19th Nov, 2019	2	35	0	37	35
	IrfanView 4.x	IrfanView	4.37	Windows32-bi	SA54959				17th Dec, 2013	1	0	0	1	1
	Mozila Firefox	Mozilla Foundation	71.x / 68.x (ESR)	Windows64-bit	SA92312		2	26 days ago	3rd Dec, 2019	3	265	0	268	32
	Mozila Firefox	Mozilla Foundation	71.x / 68.x (ESR)	Windows32-bit	SA92312		2	26 days ago	3rd Dec, 2019	11	136	0	147	74
	Mozilla SeaMonkey	Mozilla Foundation	2.49.5	Windows32-bit	SA90896		12	3 months ago	4th Sep, 2019	6	3	0	9	9
	Mozilla Thunderbird	Mozilla Foundation	68.x	Windows32-bit	SA91698		5	4 months ago	24th Oct, 2019	8	16	0	24	21
	Winamp 5.x	Nullsoft	5.63	Windows32-bi	SA46624			1 month ago	21st Jun, 2012	1	0	0	1	1
	4													
	14 4 Page 1 0	12 🕨 🕅											Displaying prod	ducts 1 - 25 of

Note • When you right click on a product or patch template in any non IE browser, you will get the below error message.

Browser Not Compatible	j
Please use IE browser and install Software Vulnerability Manager Plugin to use this feature.	

CVE Number as Criteria in Host Smart Groups

In Software Vulnerability Manager 2019, you can add CVE Number as a separate criteria while configuring New Host Smart Group:

To create a New Host Smart Groups, select the **Results >> Host Smart Groups >> Overview & Configuration**. List of existing smart group appears.

Click Create New Smart Group button. Configure New smart Group wizard appears.

In the **Criteria** section, you can add CVE Number as shown below:

🛐 Software Vulnerability Mar	nager									? Help	E Logout
Menu 📧											
Cashboard	Create New	Smart Group									Export 👻
	Name 🔿	Descri	ption	Business Impact	Compilation	Data Last Compiled	Modified Date	Averag	e Score	Hosts	Installations
Scanning	14thMarchTo				Complete	8th Dec, 2019 12:44	14th Mar, 2019 15:23		77%	2	105
		onfigure New Smart C	roup					×	73%	5	392
a Results	>2days	Smart Group Name:						_		37	4872
# Host Smart Groups	All Hosts		Enter an (optional) description fo					_		85	7644
Overview & Configuration	Aug3rdWe CSI=MAC	Description:	enter an (optional) description to	r this Smart Group						1 6	234
 Configured Host Groups (10) Product Smart Groups 	KBArticle	Business Impact:	Critical 👻						74%	14	726
Overview & Configuration	oct9_zerol	Contains hosts that ma		iteria:					73%	15	1020
Configured Product Groups (22)	products	Criteria	of the following th	real no.						37	4872
Advisory Smart Groups Overview & Configuration	venkat	Criteria							78%	3128	428794
 Configured Advisory Groups (8) 		System Score	✓ is at least	✓ 80			+				
Zero-Day Advisories (58)		System Score									
Reporting		C System Platform									
rapidong		Last Scan Date	mid will always show the	"Name" column for each host. Us	e this form to control	which additional columns ar	e shown in the orid view				
Patching		Site Name	olumn description.				e anomin in one gran nem				
		Missing KB Article	istom								
Administration		CVE Number									
4		Operating System	Scan 🕑 Insecure	CEnd-Of-Life Secure	✓ Total Site I	Name 🕑 Scan Engine	Software Platform				
Configuration								_			
								_			
							Save Ci	lose			
	14 4 Pa	ge 1 of 1 > >	11.20							Displaying Host Sr	mart Groups 1 - 10 of 10
Active Scup Threader - Interfers	m londed on: 0	th Dec. 2019 17:01							hmd12	Build	101201

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager 2019:

Issue	Description
IOJ-1921584	SG Notification throws unexpected error if SG having special characters in its name is selected .
IOJ-2079064	Unexpected error while creating a smart group by using a template.

Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at https://flexeracommunity.force.com/customer/ideas/ideaList.apexp.

System Requirements

To use the Software Vulnerability Manager 2019 console, your system should meet the following requirements:

- Minimum resolution: 1280x1024
- Internet Explorer 11 or higher (Scan results can also be viewed from other browsers)
- Internet connection capable of connecting to https://csi7.secunia.com
- The following addresses should be white-listed in the Firewall/Proxy configuration:
 - New CRL distribution URLs:
 - http://*.amazontrust.com
 - http://s.ss2.us
 - If you require explicit URLs then allow below URLs:
 - http://crl.rootca1.amazontrust.com
 - http://crl.sca1b.amazontrust.com
 - http://crl.rootg2.amazontrust.com
 - http://s.ss2.us
 - Product URLs:
 - https://csi7.secunia.com
 - https://agent.csi7.secunia.com
 - https://dl.csi7.secunia.com
 - https://*.secunia.com
 - TimeStamp URL:
 - http://timestamp.digicert.com

Note • We recommend whitelisting by domain name (timestamp.digicert.com), but if you are required to whitelist by IP, the IP address will be: 216.168.244.9.

- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

Legal Information

Copyright Notice

Copyright © 2019 Flexera.

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/ company/about/intellectual-property/. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.