



Endpoint Security Cloud - Vulnerability and Patch Management

What is Vulnerability and Patch Management?

VULNERABILITY

Most modern software will contain vulnerabilities at some point in their life cycle; either software defects that require patches to remedy, or configuration issues that require administrative activity to resolve.

PATCHING

Patching is the process of applying updates from software developers, hardware suppliers and vendors, to either enhance functionality or to improve security. This is one of the most important things you can do to mitigate vulnerabilities.

What steps does Vulnerability Patch Management follow

- First, we monitor the device for applications and any patches that these applications may require.
- Secondly, we report these vulnerabilities back to the administrator categorize them into Critical, Important, Moderate or Low. This also provides the admin with in-depth knowledge about the specific vulnerability.
- Thirdly, we provide the administrator with the ability to update the application with the latest patch to fix the security issue.
- We can also allow the administrator with the ability for VIPRE to schedule when updates will be done and update patches on next machine startup.

New Tabs

2 Additional Tabs added to the left-hand side of admin portal



New Policies Settings

The screenshot shows the 'Default Enterprise' interface with the 'Patching' tab selected in the left sidebar. The main content area is divided into two sections: 'Application Scanning' and 'Application Updates'. Both sections have a green checkmark indicating they are enabled. Below these sections is the 'APPLICATIONS' section, which includes radio buttons for 'All Supported', 'Only these...', and 'All except these...'. The 'All Supported' option is selected. A search bar labeled 'Search Apps' is highlighted with an orange box. Below the search bar is a list of 'SUPPORTED APPLICATIONS' with a pagination control showing pages 1 through 5. The 'Patching' tab in the sidebar is also highlighted with an orange box.

Default Enterprise reset cancel Save

Summary
Agent
Scanning
Active Protection
Web/DNS Protection
Web Access Control
Email Protection
Threat Handling
Patching
Firewall
IDS

Application Scanning Enable Application Scans... AGENT VERSION 12.3+
This feature will allow you to run scans looking for application vulnerabilities.

Application Updates Enable Automatic Application Updates... AGENT VERSION 12.3+
This feature will allow you to schedule automatic updates for supported applications.

APPLICATIONS
 All Supported Only these... All except these...

All applications will be updated

Search Apps

SUPPORTED APPLICATIONS -

- Adobe Systems Inc. Adobe Acrobat DC Classic 2015
- Adobe Systems Inc. Adobe Acrobat DC Classic 2017
- Adobe Systems Inc. Adobe Acrobat DC Classic 2020
- Adobe Systems Inc. Adobe Acrobat DC Continuous
- Adobe Systems Inc. Adobe Acrobat Reader DC Classic 2015
- Adobe Systems Inc. Adobe Acrobat Reader DC Classic 2017
- Adobe Systems Inc. Adobe Acrobat Reader DC Classic 2020
- Adobe Systems Inc. Adobe Acrobat Reader DC Continuous
- Alexander Roshal WinRAR
- Amazon.com Amazon Corretto

< 1 2 3 4 5 >

SCHEDULE
 Update anytime
 Update at specific times...

New Patching Tab added within the policies management page.

This is where Admins can enable the scanning and automatic application updates.

You can also use the search function to check what applications are covered. Currently 68.

Additional Vulnerabilities reporting and details pages

Using the Vulnerabilities tab we check all the current active vulnerabilities and drill down to see the specific issues in the software.

Vulnerabilities

Ungrouped | Grouped by ID | Grouped by Device

Show Last 30 days

VULNERABILITIES IN LAST 30 DAYS

386 Opened | 500 Closed

11 Devices with Vulnerabilities | 21 Currently Open

Filter: CVSS Score | Vendor | Product | Status

VULNERABILITY ID	CVSS SCORE	VENDOR	PRODUCT	DEVICE	CREATED	LAST UPDATED	STATUS
<input type="checkbox"/> CVE-2020-0607	4.3 - Important	Adobe	Acrobat	SE-SBH-RDP	03-04-2021	06-21-2021	Open
<input type="checkbox"/> CVE-2020-0607	4.3 - Important	Adobe	Acrobat	AB-SBH-RDP	03-06-2021	06-21-2021	Open
<input type="checkbox"/> CVE-2017-8592	8.8 - Critical	Microsoft	Edge	CD-SBH-RDP	03-06-2021	06-21-2021	6-15-2021
<input type="checkbox"/> CVE-2017-8592	8.8 - Critical	Microsoft	Edge	SE-SBH-RDP	04-21-2021	06-21-2021	6-15-2021

Drill down to see the specific issues in the software and update directly from this page.

Vulnerability Details

CVE-2021-38503

The frame sandbox rules were not correctly applied to XSLT stylesheets, allowing an attacker to bypass restrictions such as executing scripts or navigating the top-level frame. This vulnerability affects Firefox < 94.0, Thunderbird < 91.3, and Firefox ESR < 91.3.

REMEDIATION: Update to Latest Version

CVSS Score: 10 | 1 Versions Affected | 2 Devices Affected

- High Confidentiality Impact**
There is total loss of confidentiality, resulting in all resources divulged to the attacker.
- High Loss of Integrity**
Total loss of integrity, or a complete loss of protection.
- High Loss of Availability**
Attacker completely denies access to device resources.
- No Access Conditions**
Specialized access conditions or mitigating circumstances do not exist.
- Authentication is Not Required**
Authentication is not required to exploit the vulnerability.
- Exploitable Remotely**
The vulnerability can be exploitable with network access.

CVE ID: CVE-863 | Publish Date: 2021-12-12 | Last Update Date: 2022-01-01

References: <https://www.mozilla.org/security/advisories/mfsa2021-50/> | https://bugzilla.mozilla.org/show_bug.cgi?id=1729017 | <https://www.mozilla.org/security/advisories/mfsa2021-48/>

Specific applications page

Applications Update to Latest

FILTER: Name Vendor Application Search

APPLICATION	INSTALLED VERSION	LATEST AVAILABLE	INSTALLED DEVICES	VULNERABILITIES ON INSTALLED VERSION	VULNERABILITIES FIXED BY LATEST VERSION	ACTION
<input type="checkbox"/> Acrobat Adobe Inc.	110.6	110.6	43	—	—	
<input type="checkbox"/> Dropbox Dropbox Inc.	68.2	70.5	3	21	21 100%	Update
<input type="checkbox"/> Dropbox Dropbox Inc.	70.1	70.5	6	4	4 100%	Update
<input type="checkbox"/> 7-Zip Igor Pavlov	21.0	21.1	5	12	12 75%	Instructions
<input type="checkbox"/> Java Oracle Inc.	8.29	8.29	6	1	0 0%	Isolate

Rather than looking at just vulnerabilities, we can also look at specific applications and what vulnerabilities they are open to across the network.

All can be easily updated directly from this page.

Additional Reports Page



Timeline of Successful updates.

- Top Applications
- Top Devices
- Top Sites
- Update Status

Additional dynamic reports page added to be able to see Devices, Applications, Versions, Site.