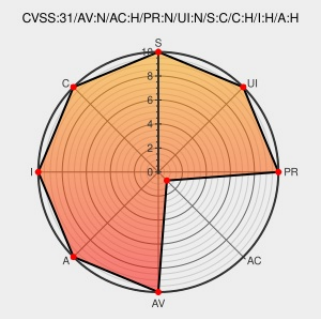
CVE-2021-3554

Published on: 11/24/2021 12:00:00 AM UTC

Last Modified on: 12/03/2021 07:25:00 PM UTC

CVE-2021-3554 - advisory for VA-9825

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Endpoint Security Tools from Bitdefender contain the following vulnerability:

Improper Access Control vulnerability in the patchesUpdate API as implemented in Bitdefender Endpoint Security Tools for Linux as a relay role allows an attacker to manipulate the remote address used for pulling patches. This issue affects: Bitdefender Endpoint Security Tools for Linux versions prior to 6.6.27.390; versions prior to 7.1.2.33. Bitdefender Unified Endpoint versions prior to 6.2.21.160. Bitdefender GravityZone versions prior to 6.24.1-1.

CVE-2021-3554 has been assigned by cve-requests@bitdefender.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Bitdefender** - **Endpoint Security Tools for Linux** version **< 6.6.27.390**

Affected Vendor/Software: **Bitdefender** - **Endpoint Security Tools for Linux** version **< 7.1.2.33**

Affected Vendor/Software: **Bitdefender** - **Unified Endpoint** version **< 6.2.21.160**

Affected Vendor/Software: **Bitdefender** - **GravityZone** version **< 6.24.1-1**

Vulnerability Patch/Work Around

An automatic update to version 6.6.27.390 fixes the issue.

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Page not found - Bitdefender	www.bitdefender.com text/html Inactive Link Not Archived	MISC www.bitdefender.com/support/security-advisories/improper-access-control-vulnerability-patchesupdate-api-va-9825

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bitdefender	Endpoint Security Tools	All	All	All	All
Application	Bitdefender	Endpoint Security Tools	All	All	All	All
Application	Bitdefender	Gravityzone	All	All	All	All
Application	Bitdefender	Gravityzone	6.24.1-1	All	All	All

cpe:2.3:a:bitdefender:endpoint_security_tools:*:*:*:*:*:*:*:*:

cpe:2.3:a:bitdefender:endpoint_security_tools:*:*:*:*:*:linux:*:*:

cpe:2.3:a:bitdefender:gravityzone:*:*:*:*:*:*:*:*:

cpe:2.3:a:bitdefender:gravityzone:6.24.1-1:*:*:*:*:*:*:*:

Discovery Credit

Nicolas VERDIER, Cybersecurity Consultant at TEHTRIS

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3554 : Improper Access Control vulnerability in the patchesUpdate API as implemented in Bitdefender Endpoi… twitter.com/i/web/status/1…	2021-11-24 15:27:21

← Previous ID Next ID→