



# 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](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H



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 **B** [cve-requests@bitdefender.com](mailto:cve-requests@bitdefender.com) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **B** [Bitdefender - Endpoint Security Tools for Linux](#) version < 6.6.27.390

Affected Vendor/Software: **B** [Bitdefender - Endpoint Security Tools for Linux](#) version < 7.1.2.33

Affected Vendor/Software: **B** [Bitdefender - Unified Endpoint](#) version < 6.2.21.160

Affected Vendor/Software: **B** [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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **7.5 - HIGH**

<b>Access Vector</b>	<b>Access Complexity</b>	<b>Authentication</b>
NETWORK	LOW	NONE
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
PARTIAL	PARTIAL	PARTIAL

## CVE References

Description	Tags	Link
Page not found - Bitdefender	<a href="http://www.bitdefender.com">www.bitdefender.com</a> <a href="#">text/html</a> <span>Inactive Link</span> <span>Not Archived</span>	<b>B</b> MISC <a href="http://www.bitdefender.com/support/security-advisories/improper-access-control-vulnerability-patchesupdate-api-va-9825">www.bitdefender.com/support/security-advisories/improper-access-control-vulnerability-patchesupdate-api-va-9825</a>
<p>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 <a href="mailto:comment@cve.report">comment@cve.report</a>.</p>		

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
<pre>cpe:2.3:a:bitdefender:endpoint_security_tools:*****:*</pre>						
<pre>cpe:2.3:a:bitdefender:endpoint_security_tools:*****:linux:*</pre>						
<pre>cpe:2.3:a:bitdefender:gravityzone:*****:*</pre>						
<pre>cpe:2.3:a:bitdefender:gravityzone:6.24.1-1:*****:*</pre>						

## 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-11-24 15:27:21

© CVE.report 2021 [🐦](#) [N](#) |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**