



# Local Privilege Escalation via Arbitrary File Operation in Bitdefender Total Security

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-7073
<b>State</b>	PUBLISHED
<b>Assigner</b>	Bitdefender
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-12-10 10:16:02 UTC
<b>Updated</b>	2026-03-31 12:16:26 UTC
<b>Description</b>	A local privilege escalation vulnerability in Bitdefender Total Security versions prior to 27.0.47.241 allows low-privileged att

## Risk And Classification

**Primary CVSS:** v4.0 8.8 HIGH from cve-requests@bitdefender.com

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000240000 probability, percentile 0.064770000 (date 2026-04-01)

**Problem Types:** CWE-59 | CWE-59 CWE-59 Improper Link Resolution Before File Access ('Link Following')

Version	Source	Type	Score	Severity	Vector
4.0	cve-requests@bitdefender.com	Secondary	8.8	HIGH	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	8.8	HIGH	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bitdefender	Antivirus	All	All	All	All
Application	Bitdefender	Antivirus Plus	All	All	All	All
Application	Bitdefender	Endpoint Security Tools	All	All	All	All

Application	Bitdefender	Internet Security	All	All	All	All
Application	Bitdefender	Total Security	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Bitdefender	Total Security	affected 27.0.47.241 custom	Windows
CNA	Bitdefender	Internet Security	affected 27.0.47.241 custom	Windows
CNA	Bitdefender	Antivirus Plus	affected 27.0.47.241 custom	Not specified

### References

Reference	Source	Link
<a href="http://www.bitdefender.com/support/security-advisories/local-privilege-escalation-via-ar...">www.bitdefender.com/support/security-advisories/local-privilege-escalation-via-ar...</a>	cve-requests@bitdefender.com	<a href="http://www.bitdefender.com">www.bitdefender.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Filip Dragovic (@filip\_dragovic) (en)

### Additional Advisory Data

Solutions

**CNA:** An automatic update to product version 27.0.47.241 fixes the issue

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)