



CVE-2021-3576

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

Summary

CVE	CVE-2021-3576
State	PUBLIC
Assigner	cve-requests@bitdefender.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-28 14:15:00 UTC
Updated	2022-04-25 18:05:00 UTC
Description	Execution with Unnecessary Privileges vulnerability in Bitdefender Endpoint Security Tools, Total Security allows a local att

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
ZDI-21-1276 Zero Day Initiative	MISC	www.zerodayi
Privilege escalation via SelpersonatePrivilege in Bitdefender Endpoint Security Tools (VA-9848) - Bitdefender	MISC	www.bitdefenc
ZDI-21-1376 Zero Day Initiative	MISC	www.zerodayi
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Zero-Day Initiative (ZDI)

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](#) 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](#)