



CVE-2020-8097

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

Summary

CVE	CVE-2020-8097
State	PUBLIC
Assigner	cve-requests@bitdefender.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-30 21:15:00 UTC
Updated	2020-09-04 16:50:00 UTC
Description	An improper authentication vulnerability in Bitdefender Endpoint Security Tools for Windows and Bitdefender Endpoint Secu

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Improper authentication vulnerability in Bitdefender Endpoint Security Tools and Endpoint Security SDK (VA-8646) - Bitdefender	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Nicolas VERDIER, Senior IT Security Consultant at Tehtris

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](#)