



CVE-2021-37852

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

Summary

CVE	CVE-2021-37852
State	PUBLIC
Assigner	security@eset.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-09 06:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	ESET products for Windows allows untrusted process to impersonate the client of a pipe, which can be leveraged by attack

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eset	Endpoint Antivirus	All	All	All	All
Application	Eset	Endpoint Security	All	All	All	All
Application	Eset	File Security	All	All	All	All
Application	Eset	Internet Security	All	All	All	All
Application	Eset	Mail Security	All	All	All	All
Application	Eset	Mail Security	All	All	All	All
Application	Eset	Nod32 Antivirus	All	All	All	All
Application	Eset	Security	All	All	All	All
Application	Eset	Server Security	8.0.12003.0	All	All	All
Application	Eset	Server Security	8.0.12003.1	All	All	All
Application	Eset	Server Security	All	All	All	All
Application	Eset	Smart Security	All	All	All	All
Application	Eset	Smart Security	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-22-148 Zero Day Initiative	MISC	www.zerodayinitiative.com	

[CA8223] Local privilege escalation vulnerability fixed in ESET products for Windows	MISC	support.eset.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

LEGACY: Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative

Legacy QID Mappings

[376449](#) ESET Endpoint Security Unnecessary Privileges Local Privilege Escalation Vulnerability

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

CVE.report and Source URL Uptime Status status.cve.report