CVE-2020-26941

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-26941
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:15:00 UTC
Updated	2021-02-02 18:34:00 UTC
Description	A local (authenticated) low-privileged user can exploit a behavior in an ESET installer to achieve arbitrary file overwrite (del

Risk And Classification

Problem Types: CWE-276

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	1294	All	All	All
Application	Eset	Internet Security	1294	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	Nod32 Antivirus	All	All	All	All
Application	Eset	Security	All	All	All	All
Application	Eset	Security	All	All	All	All
Application	Eset	Smart 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
[CA7794] Local privilege escalation vulnerability fixed in ESET products for Windows	MISC	support.eset.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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