



# CVE-2020-26941

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

## Summary

<b>CVE</b>	CVE-2020-26941
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-01-26 18:15:00 UTC
<b>Updated</b>	2021-02-02 18:34:00 UTC
<b>Description</b>	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	<a href="#">Eset</a>	<a href="#">Endpoint Antivirus</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Endpoint Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">File Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Internet Security</a>	1294	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Internet Security</a>	1294	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Internet Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Mail Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Mail Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Nod32 Antivirus</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Nod32 Antivirus</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	All	All	All	All
Application	<a href="#">Eset</a>	<a href="#">Smart Security</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[CA7794] Local privilege escalation vulnerability fixed in ESET products for Windows	MISC	<a href="https://support.eset.com">support.eset.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [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](https://mitre.org/licenses).

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