[CA8223] Local privilege escalation vulnerability fixed in ESET products for Windows

2022-01-31 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2022-0004
January 31, 2022
Severity: High

Summary

A report of a potential local privilege escalation vulnerability was submitted to ESET by the Zero Day Initiative (ZDI). It potentially allows an attacker to misuse the AMSI scanning feature in specific cases. ESET mitigated the issue and recommends using the most recently released product versions, as detailed below.

Details

On November 18, 2021, ESET became aware of a potential vulnerability of local privilege escalation in its products for Windows. According to the report, submitted by the Zero Day Initiative (ZDI), an attacker who is able to get `SeImpersonatePrivilege` can misuse the AMSI scanning feature to elevate to `NT AUTHORITY\SYSTEM` in some cases. The `SeImpersonatePrivilege` is by default available to the local Administrators group and the device's Local Service accounts, which are already highly privileged and thus limit the impact of this vulnerability.

ESET investigated and verified this report and prepared new builds of its products that are not susceptible to this vulnerability.

The CVE ID reserved by ESET for this vulnerability is CVE-2021-37852 with the following CVSS v3 vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

To the best of our knowledge, there are no existing exploits that take advantage of this vulnerability in the wild.

Solution

ESET prepared the following fixed product versions that are not susceptible to the vulnerability and recommends that users upgrade to them as soon as possible:

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security and ESET Smart Security 15.0.19.0 (released on December 8, 2021)
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 9.0.2032.6 and 9.0.2032.7 (released on December 16, 2021)
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 8.0.2028.3, 8.0.2028.4, 8.0.2039.3, 8.0.2039.4, 8.0.2044.3, 8.0.2044.4, 8.1.2031.3, 8.1.2031.4, 8.1.2037.9 and 8.1.2037.10 (released on January 25, 2022)
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 7.3.2055.0 and 7.3.2055.1 (released on January 31, 2022)
- ESET Server Security for Microsoft Windows Server 8.0.12010.0 (released on December 16, 2021)
- ESET File Security for Microsoft Windows Server 7.3.12008.0 (released on January 12, 2022)
- ESET Security for Microsoft SharePoint Server 8.0.15006.0 (released on December 16, 2021)
- ESET Security for Microsoft SharePoint Server 7.3.15002.0 (released on January 12, 2022)
- ESET Mail Security for IBM Domino 8.0.14006.0 (released on December 16, 2021)
- ESET Mail Security for IBM Domino 7.3.14003.0 (released on January 26, 2021)
- ESET Mail Security for Microsoft Exchange Server 8.0.10018.0 (released on December 16, 2021)
- ESET Mail Security for Microsoft Exchange Server 7.3.10014.0 (released on January 26, 2022)

Users of ESET Server Security for Microsoft Azure are advised to upgrade ESET File Security for Microsoft Azure to the latest version of ESET Server Security for Microsoft Windows Server.

An alternative way to eliminate attack surface

> **An alternative way to eliminate attack surface**
> The attack surface can also be eliminated by disabling the **Enable advanced scanning via AMSI** option in ESET products' Advanced setup.
>
> However, ESET strongly recommends performing an upgrade to a fixed product version and only applying this workaround when the upgrade is not possible for an important reason.

The following product versions are susceptible to the vulnerability when running on Windows 10 and later or Windows Server 2016 and later:

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security and ESET Smart Security Premium from version 10.0.337.1 to 15.0.18.0
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows from version 6.6.2046.0 to 9.0.2032.4
- ESET Server Security for Microsoft Windows Server 8.0.12003.0 and 8.0.12003.1, ESET File Security for Microsoft Windows Server from version 7.0.12014.0 to 7.3.12006.0
- ESET Server Security for Microsoft Azure from version 7.0.12016.1002 to 7.2.12004.1000
- ESET Security for Microsoft SharePoint Server from version 7.0.15008.0 to 8.0.15004.0
- ESET Mail Security for IBM Domino from version 7.0.14008.0 to 8.0.14004.0
- ESET Mail Security for Microsoft Exchange Server from version 7.0.10019 to 8.0.10016.0

Feedback & Support

If you have feedback or questions about this issue, contact us using the ESET Security Forum, or via local ESET Technical Support.

Acknowledgment

ESET values the principles of responsible disclosure within the security industry and would like to express our thanks to Trend Micro's Zero Day Initiative team, and specifically Michael DePlante (@izobashi) who reported this issue.

Version log

Version 1.0 (January 31, 2022): Initial version of this document