ESET Tech Center

ESET Customer Advisory: Unquoted path privilege vulnerability in ESET products for Windows fixed

2024-01-30 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2024-0002

January 26, 2024

Severity: Low

Summary

ESET received a report for an unquoted path privilege vulnerability in its products for Windows. Fixed product versions are available to download, and we recommend upgrading or scheduling upgrades.

Details

A report received by ESET outlined a possible unquoted path privilege attack, exploiting the path to the ESET Forwarder (efwd.exe) service that was stored in the registry without being enclosed in quotes. This would allow an attacker to drop a prepared program to a specific location on a disk and have it run on boot with the permission set of the user running the service, which was **NT AUTHORITY\NetworkService**, therefore not escalating their privileges. This attack was possible only immediately after an upgrade from a previous ESET product version, not during regular product use or after a fresh product installation.

ESET remedied this possible attack vector and has prepared new builds of its products that are not susceptible to this vulnerability.

The reserved CVE ID for this vulnerability is CVE-2023-7043. ESET evaluated the severity of this vulnerability as low, and the CVSS v3.1 base score is 3.3 with the following vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

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

Solution

ESET prepared fixed builds of its consumer, business and server products, and we recommend upgrading now or scheduling the upgrades shortly. The fixed builds are available in the Download section of www.eset.com or via the ESET Repository.

This issue is **resolved** in the following builds:

- ESET Endpoint Security and ESET Endpoint Antivirus 11.0.2032.x and later
- ESET NOD32 Antivirus, ESET Internet Security and ESET Smart Security Premium

17.0.15.0 and later

- ESET Mail Security for Microsoft Exchange Server 10.1.10014.0 and later

Affected programs and versions

- ESET Endpoint Security and ESET Endpoint Antivirus 10.1.2046.x–10.1.2063.x
- ESET NOD32 Antivirus, ESET Internet Security and ESET Smart Security Premium 16.1.14.0–16.2.15.0
- ESET Mail Security for Microsoft Exchange Server 10.1.10012.0

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 Tom Ussher.

Version log

Version 1.0 (January 26, 2024): Initial version of this document