Denial of Service Vulnerability in ESET products for Windows fixed

2024-07-15 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2024-0010

July 12, 2024

Severity: Medium

Summary

A report of a denial of service vulnerability was submitted to ESET by Ali Jammal of Deloitte Netherlands and Alaa Kachouh of Mastercard. The vulnerability, present shortly after product installation or upgrade, potentially allowed an attacker to render ESET's security product inoperable, provided non-default preconditions were met. ESET mitigated this by preparing fixed versions of its security products.

Details

On systems with an affected product installed, incorrect access permissions could, under specific conditions, allow an attacker to delete certain files required for the product to provide protection. This would cause the product to become inoperable after the next reboot.

The incorrect access permissions could only be misused during the product initialization phase, shortly after the product installation or manual upgrade to a higher version via an installation file, provided the installation file did not include all product modules. Once the product was installed and its modules were downloaded and initialized, it was not possible to delete the files anymore, as they were protected by the ESET Self-Defense feature. Additionally, upgrading the product to a higher version via the built-in automatic upgrade option did not expose the system to this vulnerability. Similarly, when using a full installation file containing the modules, there was no period after the installation when the files could be deleted, as the ESET Self-Defense feature started immediately. Moreover, the vulnerability could only be exploited if the product had initially been installed to a custom (non-default) path.

The reserved CVE ID for this vulnerability is CVE-2024-3779, the CVSS v3.1 score is 6.1 with the following CVSS vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

To the best of our knowledge, this vulnerability has not been exploited in the wild.

Solution

ESET prepared fixed builds of its consumer, business and server security products for the

Windows operating system and recommends upgrading to these or scheduling the upgrades in the near future. The fixed builds are available in the Download section of www.eset.com or via the ESET Repository.

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 17.2.7.0 and later
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 11.1.2039.0 and later
- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server) 11.0.12012.0 and later
- ESET Mail Security for Microsoft Exchange Server 11.0.10008.0 and later
- ESET Security for Microsoft SharePoint Server 11.0.15004.0 and later

Note
Fixed versions

At the time of the release of this advisory, builds from the most recent product versions were fixed and released. In accordance with ESET's End of Life policy, previous versions in Full Support or Limited Support will see their fixed builds released in their regular service release slots, should those be planned for the respective product versions.

Affected programs and versions

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 17.1.13.0 and earlier
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 11.0.2044.0 and earlier
- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server) 11.0.12011.0 and earlier
- ESET Mail Security for Microsoft Exchange Server 11.0.10005.0 and earlier
- ESET Mail Security for IBM Domino
- ESET Security for Microsoft SharePoint Server 11.0.15002.0 and earlier

Note
End of Life product versions

ESET product versions that have reached End of Life are not listed.

Feedback & Support

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

Acknowledgment

ESET values the principles of coordinated disclosure within the security industry and would like to express our thanks to Ali Jammal of Deloitte Netherlands and Alaa Kachouh of Mastercard.