## ESET Customer Advisory: Link Following Local Privilege Escalation Vulnerability in ESET products for Windows fixed


2024-02-14 - Steef | ESET Nederland - Reacties (0) - Customer Advisories


ESET Customer Advisory 2024-0003

February 14, 2024

Severity: High

### Summary


A report of a local privilege escalation vulnerability was submitted to ESET by the Zero Day Initiative (ZDI). The vulnerability potentially allowed an attacker to misuse ESET's file operations, as performed by the Real-time file system protection, to delete files without having proper permission.


### Details

The vulnerability in file operations handling, performed by the Real-time file system protection feature on the Windows operating system, potentially allowed an attacker with an ability to execute low-privileged code on the target system to delete arbitrary files as NT AUTHORITY\SYSTEM, escalating their privileges.

The reserved CVE ID for this vulnerability is CVE-2024-0353. The CVSS v3.1 score is 7.8 with the following CVSS vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 or via the ESET Repository.

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 17.0.10.0 and later
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 11.0.2032.0, 10.1.2063.0, 10.0.2052.0, 9.1.2071.0, 8.1.2062.0 and later from the respective version family
- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server) 10.0.12015.0, 9.0.12019.0, 8.0.12016.0, 7.3.12013.0 and later from

the respective version family

- ESET Mail Security for Microsoft Exchange Server 10.1.10014.0, 10.0.10018.0, 9.0.10012.0, 8.0.10024.0, 7.3.10018.0 and later from the respective version family
- ESET Mail Security for IBM Domino 10.0.14007.0, 9.0.14008.0, 8.0.14014.0, 7.3.14006.0 and later from the respective version family
- ESET Security for Microsoft SharePoint Server 10.0.15005.0, 9.0.15006.0, 8.0.15012.0, 7.3.15006.0 and later from the respective version family
- ESET File Security for Microsoft Azure customers should migrate to the latest version of ESET Server Security for Microsoft Windows Server

## Affected programs and versions

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 16.2.15.0 and earlier
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 10.1.2058.0, 10.0.2049.0, 9.1.2066.0, 8.1.2052.0 and earlier from the respective version family
- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server) 10.0.12014.0, 9.0.12018.0, 8.0.12015.0, 7.3.12011.0 and earlier from the respective version family
- ESET Mail Security for Microsoft Exchange Server 10.1.10010.0, 10.0.10017.0, 9.0.10011.0, 8.0.10022.0, 7.3.10014.0 and earlier from the respective version family
- ESET Mail Security for IBM Domino 10.0.14006.0, 9.0.14007.0, 8.0.14010.0, 7.3.14004.0 and earlier from the respective version family
- ESET Security for Microsoft SharePoint Server 10.0.15004.0, 9.0.15005.0, 8.0.15011.0, 7.3.15004.0 and earlier from the respective version family
- ESET File Security for Microsoft Azure (all versions)

NOTE: 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 Nicholas Zubrisky and Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative.