DLL Search Order Hijacking Vulnerability in ESET products for Windows fixed

2025-04-04 - Steef | ESET Nederland - Comments (0) - Customer Advisories

DLL Search Order Hijacking Vulnerability in ESET products for Windows fixed

ESET Customer Advisory 2025-0004

April 4, 2025

Severity: High

Summary

A report of a DLL search order hijacking vulnerability was submitted to ESET by Andrei Gunkin from Kaspersky. The vulnerability potentially allowed an attacker with administrator privileges to load a malicious dynamic-link library and execute its code. ESET mitigated this by preparing fixed versions of its security products.

Details

On systems with an affected ESET product installed, an attacker could plant a malicious dynamic-link library to a specific folder and execute its content by running ESET Command Line Scanner, which would load the planted library instead of the intended system library.

This technique did not elevate the privileges, though—the attacker would retain the privileges under which they ran the executable.

The reserved CVE ID for this vulnerability is CVE-2024-11859, the CVSS v4.0 score is 8.4 with the following CVSS vector: AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

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 ESET Repository.

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 18.1.10.0 and later
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 12.0.2045.0, 11.1.2059.0 and later from the respective version family
- ESET Small Business Security and ESET Safe Server 18.1.10.0 and later
- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server) 11.1.12009.0 and later
- ESET Mail Security for Microsoft Exchange Server 11.1.10011.0, 11.0.10010.0, 10.1.10017.0 and later from the respective version family
- ESET Security for Microsoft SharePoint Server 11.1.15003.0, 11.0.15007.0, 10.0.15008.0 and later from the respective version family

Affected products

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 18.0.12.0 and earlier
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows 12.0.2038.0, 11.1.2053.2 and earlier from the respective version family
- ESET Small Business Security and ESET Safe Server 18.0.12.0 and earlier
- ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server) 11.1.12005.2 and earlier
- ESET Mail Security for Microsoft Exchange Server 11.1.10008.0, 11.0.10008.0, 10.1.10014.0 and earlier from the respective version family
- ESET Security for Microsoft SharePoint Server 11.1.15001.0, 11.0.15004.0, 10.0.15005.1 and earlier from the respective version family

Note

ESET product versions that no longer receive hotfixes according to the End of Life policy may not be listed.

Feedback & Support

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

Acknowledgment

ESET values the principles of coordinated disclosure within the security industry and would like to express our thanks to Andrey Gunkin from Kaspersky.

Version log

- Version 1.1 (April 16, 2025): Clarification regarding the required privileges; updated score, vector and severity
- Version 1.0 (April 4, 2025): Initial version of this document