مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in ESET Products

Tracking #:432315620

Date:16-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity vulnerability in ESET Products that could be exploited to gain unauthorised access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-0353**
- **CVSS v3.1 score 7.8 High**
- A local privilege escalation vulnerability exists in ESET security products, potentially allowing attackers to misuse ESET's file operations to delete files without proper permissions.
- This vulnerability in the real-time file system protection feature, which handles file operations. An attacker with low privileges could exploit this vulnerability to delete arbitrary files with System privileges

Affected Products 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)

Fixed Versions:

- 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 migrate to the latest version of ESET Server Security for Microsoft Windows Server

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by ESET.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://support.eset.com/en/ca8612-eset-customer-advisory-link-following-local-privilege-escalation-vulnerability-in-eset-products-for-windows-fixed