مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

ESET Local Privilege Escalation Vulnerabilities

Tracking #:432316320

Date:24-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed ESET has released patches addressing two local privilege escalation vulnerabilities identified in its products for Windows and macOS operating systems.

TECHNICAL DETAILS:

ESET has released patches addressing two local privilege escalation vulnerabilities identified in its products for Windows and macOS operating systems. The vulnerabilities, tracked as CVE-2024-7400 and CVE-2024-6654, allow attackers to exploit ESET's file operations, potentially leading to unauthorized file deletions and denial-of-service conditions. Users are advised to ensure their products are updated to the latest versions to mitigate these risks. ESET has stated that it is not aware of any public exploits for these vulnerabilities at this time.

Vulnerability Details:

1. **CVE-2024-7400 (Windows)**

- CVSS Score: 7.3 (High)
- Description: This vulnerability allows an attacker with low privileges to misuse ESET's file operations during the removal of detected files, enabling them to delete arbitrary files without proper permissions.
- Affected products:
  - ESET Small Business Security and ESET Safe Server
  - ESET Endpoint Antivirus and ESET Endpoint Security for Windows
  - ESET Server Security for Windows Server (formerly File Security for Microsoft Windows Server)
  - ESET Mail Security for Microsoft Exchange Server
  - ESET Mail Security for IBM Domino
  - ESET Security for Microsoft SharePoint Server
  - ESET File Security for Microsoft Azure
- Fix: Resolved in Cleaner module 1251

2. **CVE-2024-6654 (macOS)**

- CVSS Score: 6.8 (Medium)
- Description: This vulnerability permits a logged-in user to perform a denial-of-service attack against ESET security products, potentially disabling them and causing system slowdowns.
- Impact: Affected products include ESET Cyber Security (versions 7.0 – 7.4.1600.0) and ESET Endpoint Antivirus for macOS (versions 7.0 – 7.5.50.0).
- Fix: Addressed in Cyber Security version 7.5.74.0 and Endpoint Security for macOS version 8.0.7200.0.

RECOMMENDATIONS:

- Immediate Action: Users of affected ESET products should ensure they are running the latest versions as per the fixes provided.
- Automatic Updates: Customers with regularly updated ESET products do not need any further action as the updates have been applied automatically.

- New Installations: For new installations, download the latest installers from the official ESET website or repository.

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:

- https://support.eset.com/en/ca8726-local-privilege-escalation-fixed-for-vulnerability-during-detected-file-removal-in-eset-products-for-windows
- https://support.eset.com/en/ca8725-local-privilege-escalation-vulnerability-in-eset-products-for-macos-fixed