ESET Customer Advisory: Improper following of a certificate's chain of trust in ESET security products fixed

2023-12-20 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2023-0015

December 20, 2023

Severity: High

Summary

ESET was made aware of a vulnerability in its SSL/TLS protocol scanning feature, which is available in ESET products listed in the Affected products section below. This vulnerability would cause a browser to trust a site with a certificate signed with an obsolete algorithm that should not be trusted.

Details

The vulnerability in the secure traffic scanning feature was caused by improper validation of the server's certificate chain. An intermediate certificate signed using the MD5 or SHA1 algorithm was considered trusted, and thus the browser on a system with the ESET secure traffic scanning feature enabled could be caused to trust a site secured with such a certificate.

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

CVE ID reserved by ESET for the vulnerability is CVE-2023-5594, the CVSS v3.1 score is 7.5 with the following CVSS vector: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:N

Solution

ESET prepared a fix and distributed it automatically in Internet protection module 1464. The module is being distributed via automatic product updates, so no user interaction is required. Distribution of the module started on November 21, 2023 for customers using the pre-release update channel, on November 27, 2023 for ESET consumer products users and on December 11, 2023 for users using ESET business and server products.

Affected products

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows
- ESET Endpoint Antivirus for Linux 10.0 and above
- ESET Server Security for Windows Server (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
- ESET Server Security for Linux 10.1 and above

Feedback & Support

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

Acknowledgement

ESET values the principles of responsible disclosure within the security industry and would like to express our thanks to the undisclosed reporter.

Version log

Version 1.0 (December 20, 2023): Initial version of this document