[CA8268] Local privilege escalation vulnerabilities in installers for ESET products for Windows fixed

2022-05-09 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2022-0009

May 9, 2022

Severity: High

Summary

ESET was made aware of two vulnerabilities in installers of its products for Windows that allow a user logged into the system to perform a privilege escalation attack by misusing the Repair and Uninstall options. ESET released an automatic module update to cover these vulnerabilities in already installed eligible products and released fixed product installers.

Details

CVE-2021-37851 allows a user who is logged into the system to perform a privilege escalation attack by exploiting the repair feature of the installer to run malicious code with higher privileges.

The CVSS v3 base score for CVE-2021-37851 is 7.3 with the following vector AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVE-2022-27167 affects the Repair and Uninstall options and exploiting it may lead to arbitrary file deletion.

The CVSS v3 base score for CVE-2022-27167 is 7.1 with the following vector AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

To the best of our knowledge, there are no existing exploits that take advantage of these vulnerabilities in the wild.

Solution

ESET released an update of the Antivirus and antispyware scanner module to cover these vulnerabilities in already installed products, which was distributed automatically. ESET also released fixed builds of its products for Windows.

Since installed products receive the patch via the Antivirus and antispyware scanner module update, users with ESET products installed do not need to take any action regarding these vulnerabilities. For new installations, we recommend using the latest installers downloaded from the ESET website or the ESET repository.

The issues are resolved in the following modules and builds:

- Antivirus and antispyware scanner module 1587 was released on March 31, 2022, for products in Full and Limited support, according to ESET's End of Life policy. Note that this module update is downloaded by ESET products automatically along with Detection Engine updates.
- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium versions 15.1.12.0
- ESET Endpoint Antivirus and ESET Endpoint Security from versions 9.0.2046.0, 8.1.2050.0 and 8.0.2053.0 respectively
- ESET Server Security for Microsoft Windows Server from version 9.0.12012.0
- ESET File Security for Microsoft Windows Server released as "ESET Server Security for Microsoft Windows Server" from version 8.0.12013.0
- ESET Mail Security for Microsoft Exchange Server from version 8.0.10020.0
- ESET Mail Security for IBM Domino from version 8.0.14011.0
- ESET Security for Microsoft SharePoint Server from version 8.0.15009.0

Note: Users of ESET Server Security for Microsoft Azure are advised to use ESET Server Security for Microsoft

Windows Server.

Affected programs and versions

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium versions from 11.2
- ESET Endpoint Antivirus and ESET Endpoint Security from version 6.0
- ESET Server Security for Microsoft Windows Server from version 8.0
- ESET File Security for Microsoft Windows Server from version 6.0
- ESET Server Security for Microsoft Azure from version 6.0
- ESET Mail Security for Microsoft Exchange Server from version 6.0
- ESET Mail Security for IBM Domino from version 6.0
- ESET Security for Microsoft SharePoint Server from version 6.0

Feedback & Support

If you have feedback or questions about this issue, contact us using 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 Brecht Snijders for reporting **CVE-2022-27167**.

Version log

Version 1.0 (May 9, 2022): Initial version of this document