Arbitrary file rewrite by unprivileged user in ESET products for macOS fixed

2019-07-16 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2019-0010
July 9, 2019
Severity: Critical

Summary

ESET was made aware of a potential vulnerability in its consumer and business products for macOS. Upon detailed inspection, ESET identified the cause of the issue and has prepared the necessary fix for the products concerned. Users may now download and install the update.

Details

ESET received a report describing a vulnerability in ESET Cyber Security, ESET Cyber Security Pro, ESET Endpoint Antivirus for macOS and ESET Endpoint Security for macOS. This vulnerability allowed an attacker to create a special symbolic link to any file, including system files in /tmp directory utilized by ESET daemon, which, if an attempt at use was made, would cause the actual file to be overwritten. This would allow the attacker to take the system out of service or to take control of it.

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

If you were not directly affected by this issue, you do not need to replace the library. The fixed library will be included in future versions of ESET Security Management Center.

Solution

ESET has prepared fixed builds of its consumer and business products for macOS and recommends to its users to download them from the Download section of www.eset.com and install them as soon as possible.

The following builds contain the fixes:

- ESET Cyber Security and ESET Cyber Security Pro 6.7.900.0 and higher (released on July 9, 2019)
- ESET Endpoint Antivirus for macOS and ESET Endpoint Security for macOS 6.7.900.0 and higher (released on July 9, 2019)

Affected programs and versions

- ESET Cyber Security and ESET Cyber Security Pro 6.7.876.0 and lower
- ESET Endpoint Antivirus for macOS and ESET Endpoint Security for macOS 6.7.876.0 and lower

Feedback & Support

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

Acknowledgement

ESET values the principles of responsible disclosure within the security industry and would like to hereby express thanks to the RACK911 Labs which reported this issue to us.

Version log

Version 1.0 (July 9, 2019): Initial version of this document