ESET Customer Advisory: Local privilege escalation via insecure temporary batch file execution in ESET Management Agent for Windows fixed

2026-02-06 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2026-0003

February 6, 2026

Severity: High

Summary

A report of a local privilege escalation vulnerability was submitted to ESET by Mahdi Hamedani Nezhad. The vulnerability potentially allowed an attacker to misuse ESET Management Agent's file operations during the execution of commands on the Windows platform to elevate the context of the executed code from Administrator to SYSTEM.

Details

The vulnerability lies in the way how file operations are handled during the execution of commands from the ESET PROTECT management console on the Microsoft Windows operating system. The commands are being stored in a predictable and writable location, therefore altering these temporary files allows an attacker with the ability to run code under Administrator privileges to change the commands and have them executed under the SYSTEM account, thus escalating their privileges. Although local Administrator access rights are required to perform this privilege escalation attack, ESET implemented multiple measures to increase the security of the ESET Management Agent file operations during the execution of commands from ESET PROTECT, which are available in the already released ESET Management Agent version 13.0.1400.0.

The CVE ID reserved for this vulnerability is CVE-2025-13818, with the CVSS v4.0 score 8.3 and the following CVSS 4.0 vector: AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

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

Solution

ESET released ESET Management Agent version 13 with improved security of the file operations performed during the execution of the commands. ESET recommends its customers using the ESET PROTECT management solution to check the ESET Management Agent version deployed on their Windows operating systems and to schedule upgrades to the latest released version, i.e. 13.0.1400.0 or newer. For new installations, we recommend using the latest installers downloaded from www.eset.com or the ESET repository.

Affected ESET products

- ESET Management Agent 12.5.2104.0 and earlier

NOTE:

ESET product versions that have reached End of Life might not be listed.

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 Mahdi Hamedani Nezhad.

Version log

Version 1.0 (January 30, 2026): Initial version of this document