ESET Customer Advisory: Local privilege escalation vulnerability fixed in ESET Inspect Connector for Windows

2026-01-30 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2026-0002

January 30, 2026

Severity: High

Summary

A report of a local privilege escalation vulnerability was submitted to ESET by Manuel Feifel of InfoGuard Labs. The vulnerability potentially allowed an attacker with low privileges to plant a custom file in a specific location, which would then cause ESET Inspect Connector to load and execute malicious code, gaining SYSTEM permissions. ESET released a fixed version of ESET Inspect Connector and recommends upgrading to it or scheduling the upgrade in the near future.

Details

The vulnerability allows a low-privileged user logged in to the system to perform a privilege escalation attack by planting a custom configuration file in a specific location, which then causes ESET Inspect Connector to load a malicious DLL file upon its launch and execute it under its process. This results in the malicious code being run with SYSTEM permissions, achieving privilege escalation.

To the best of our knowledge, no exploits exist in the wild that abuse this vulnerability.

The CVE ID reserved for this vulnerability is CVE-2025-13176, with the CVSS v4.0 score 8.4 and the following vector: AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N.

Solution

ESET prepared a fixed build of ESET Inspect Connector that is no longer susceptible to this vulnerability and recommends upgrading to it or scheduling the upgrade in the near future. The fixed build is available in the Download section of www.eset.com or via ESET Repository as well.

- ESET Inspect Connector 3.0.5765 and later, running on Windows OS

Affected ESET products

- ESET Inspect Connector 2.8.5555 and earlier, running on Windows OS

Feedback & Support

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

Acknowledgement

ESET values the principles of coordinated disclosure within the security industry and would like to express our

thanks to Manuel Feifel (@p0w1_) of InfoGuard Labs.

Version log

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