ESET Customer Advisory: Local privilege escalation via unauthenticated ALPC in ESET Inspect Connector for Windows fixed

2026-07-15 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2026-0011

July 14, 2026

Severity: High

Summary

A local privilege escalation vulnerability in ESET Inspect Connector was discovered internally by ESET's Joan Calvet. The vulnerability was caused by improper authentication in an IPC channel. ESET mitigated this by preparing a fixed version of the affected product.

Details

On systems with the affected ESET product installed, an attacker could send self-crafted Advanced Local Procedure Call (ALPC) requests to the vulnerable process' interface. Without proper authentication or origin validation in place, this message would be accepted and processed, enabling the attacker to access restricted functionality.

The reserved CVE ID for this vulnerability is CVE-2026-6423, the CVSS v4.0 score is 8.5 with the following vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Solution

ESET prepared fixed builds of the affected product and recommends upgrading to these or scheduling the upgrades in the near future. The fixed builds are available to download from www.eset.com or via ESET Repository.

- ESET Inspect Connector 3.1.6017.0 (and later) for Windows

Affected products

- ESET Inspect Connector 3.0.5775.0 (and earlier) for Windows

NOTE: ESET product versions that no longer receive hotfixes according to the End of Life policy may not be listed.

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.

Reporting security vulnerabilities to ESET

ESET welcomes reports of security vulnerabilities in its products. See http://www.eset.com/int/security-vulnerability-reporting/

Version log

Version 1.0 (July 14, 2026): Initial version of this document