ESET Customer Advisory: Denial-of-service vulnerability in ESET PROTECT On-Prem fixed

2025-08-25 - Steef | ESET Nederland - Reacties (0) - Customer Advisories

ESET Customer Advisory 2025-0014

August 22, 2025

Severity: Medium

Summary

During the impact assessment of CVE-2025-48976 and CVE-2025-48988, ESET developers found a similar issue in the ESET PROTECT On-Prem Web Console code. ESET released fixed versions of ESET PROTECT On-prem and recommends upgrading to these or scheduling the upgrades in the near future.

NOTE:

ESET PROTECT, hosted as a cloud service by ESET, was not affected.

Details

The vulnerability lies in the missing limits on the input data for multipart requests. Specifically crafted requests to upload servlets to the ESET PROTECT On-Prem Web Console might cause increased resource consumption (CPU and RAM), leading to conditions for a Denial-of-Service attack, for instance, preventing the correct functioning of the ESET PROTECT Web Console (and possibly other services running on the same server).

NOTE: Installed ESET security products continue to protect the systems where they are deployed, even when it is temporarily impossible to manage them via ESET PROTECT.

The CVE ID reserved for this vulnerability is CVE-2025-8352, with the CVSS v4.0 score 6.9 and the following CVSS vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

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

Solution

ESET removed the vulnerable code and used the implementation provided by Apache Tomcat instead.

ESET released fixed builds of ESET PROTECT On-Prem in version families 12.1, 12.0, and 11.1 and recommends upgrading to these or scheduling the upgrades in the near future.

The fixed builds (listed below) are available in the Download section of www.eset.com or via the ESET Repository.

- ESET PROTECT On-Prem 12.1.11.0 using Web Console 12.1.260.0 on Apache Tomcat 9.0.107
- ESET PROTECT On-Prem 12.0.15.0 using Web Console 12.0.306.0 on Apache Tomcat 9.0.107
- ESET PROTECT On-Prem 11.1.18.0 using Web Console 11.1.159.0 on Apache Tomcat 9.0.107

NOTE:

Web Console in the above-listed versions in the Virtual Appliance contains the fix for this vulnerability.

However, Apache Tomcat versioning on Linux does not match the versioning on the Windows platform. Those releases are handled by the respective maintainer of the repository of the given OS, so customers using the ESET PROTECT Virtual Appliance and those who deployed ESET PROTECT On-Prem on Linux themselves should check the deployed Apache Tomcat version and, when available, upgrade to a version with the CVE-2025-48976 and CVE-2025-48988 vulnerabilities fixed.

For new installations, we recommend using the latest installers downloaded from www.eset.com or the ESET repository.

Affected ESET products

- ESET PROTECT On-Prem 12.1.9.0 (with Web Console 12.1.252.0) and earlier
- ESET PROTECT On-Prem 12.0.13.0 (with Web Console 12.0.289.0) and earlier
- ESET PROTECT On-Prem 11.1.16.0 (with Web Console 11.1.149.0) and earlier

NOTE:

ESET product versions that have reached End of Life or Limited Support 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.

Version log

Version 1.0 (August 22, 2025): Initial version of this document