[CA7633] False positives in ESET Enterprise Inspector fixed

2020-10-02 - Mitchell | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2020-0014
October 1, 2020
Severity: Minor

Summary

ESET recently discovered an increasing number of false positive alarms in ESET Enterprise Inspector. Upon investigation, a fixed module was prepared and will be released soon.

Details

It has come to ESET's attention, via both internal and external sources, that ESET Enterprise Inspector consoles started to report an increase in false positive alarms, such as "Injection into browser process", coming from various executables. The alarms may have also been received in duplicate.

After immediate investigation, ESET found that this behavior was caused by two recently added attack type detections related to code injection.

Solution

A fix was prepared in the form of updated HIPS support module, version 1401. It was distributed to customers using the pre-release updates on September 30 and a full roll-out will follow in the coming days. The module is loaded by the product automatically, thus no action is necessary from the customers' side.

Affected products

ESET Enterprise Inspector