Security advisory

Remote Code Execution

October, 2023

CVE-2023-41630
Release date: 07/09/2023
Department: POST Cyberforce
Pianezzola Thomas

Vulnerability summary

Product	eSST Monitoring
Product homepage	https://esst.lu
Affected product versions	2.147.1 and below
Severity	Critical - CVSS v3.1 score: 10
CVSS v3.1	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE	CWE-1104
Workarounds	In progress

Validated impact:

Unauthenticated Remote Code Execution

Timeline

Date	Action
27 07 2023	Vulnerability identification, exploitation and impact validation
27 07 2023	Vendor notified and acknowledged the vulnerability
31 08 2023	CVE-2023-41630 assigned by MITRE
07 09 2023	Vendor informed about assigned CVE id

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41630
- https://cwe.mitre.org/data/definitions/1104.html
- https://github.com/yiisoft/yii2-gii/issues/433
- https://lab.wallarm.com/yii2-gii-remote-code-execution/

Product description

eSST monitoring can be used to train, prevent, advise or support employers, resource persons or designated workers.

Advisory

The usage of outdated and vulnerable component (Gii code generator from Yii PHP Framework) led to Remote Code Execution (RCE).

Vulnerability description

It is possible to inject PHP code that will be executed server side from an unauthenticated point of view.

Vulnerable endpoints:

Gii Code Generator deployed on `/gii/default/*`

Proof of concept

Check access to the code generator at `/gii/default/index`

Recommendation

`Contact eSST to receive the patched version of the software.`