EGI SVG Advisories

Advisory-EGI-SVG-2025-09

CRITICAL risk FTS3 Web Monitoring Security Vulnerability

Date: 2025-06-26
Updated: 2025-07-30

CRITICAL risk vulnerability concerning “blind” SQL injection involving the FTS3 Web Monitoring software via the `/linkinfo` endpoint, allowing database access to the attacker. [R 1]

IDs AND CVSS SCORE

EGI SVG ID : EGI-SVG-2025-09

CVE ID : N/A

AFFECTED SOFTWARE AND VERSIONS

This is fixed in version fts-monitoring-3.14.1-1 and backported via fts-monitoring-3.13.3-1

ACTIONS REQUIRED/RECOMMENDED

Sites running FTS3 Web monitoring are required to update urgently, using information in references below.

All running resources MUST be either patched or have mitigation in place or software removed by 2025-07-04 00:00 UTC

Sites failing to act and/or failing to respond to requests from the EGI CSIRT team risk site suspension.

In addition, the FTS team recommends the followings [R 1]:

- Consider all stored credentials in the database as exposed;

- Upgrade to the latest patched version;
- Regenerate all Cloud Credentials stored;
- Regenerate all Token Provider client secrets;

STATUS OF THIS ADVISORY

TLP:CLEAR information - Unlimited distribution

https://advisories.egi.eu/Advisory-EGI-SVG-2025-09

Minor updates may be made without re-distribution to the sites.

CONTACT AND OTHER INFORMATION ON SVG

```
This advisory is subject to the Creative Commons licence
https://creativecommons.org/licenses/by/4.0/ and
the EGI (https://www.egi.eu/) Software Vulnerability Group
must be credited. --
```

Comments or questions should be sent to svg-rat at mailman.egi.eu

Vulnerabilities relevant for EGI can be reported at report-vulnerability at egi.eu

(see [R 99] for further details, and other information on SVG)

REFERENCES

- [R 1] https://cernbox.cern.ch/s/fE6sycaKFsv0u7U
- [R 2] https://fts.web.cern.ch/fts/
- [R 3] https://fts3-docs.web.cern.ch/fts3-docs/docs/install/quick.html#decide-which-version-to-use
- [R 4] https://fts-repo.web.cern.ch/fts-repo/el9/x86_64/
- [R 99] https://confluence.egi.eu/display/EGIBG/SVG+Advisories

CREDITS

SVG was alerted to this vulnerability by Pau Cutrina

This site is open source. Improve this page.