SERVICE FACTS on SECURITY NOTICE

FUJITSU ETERNUS CS8000 (CONTROL CENTER) VULNERABILITIES

(PSS-IS-2022-050316)

Affected component(s):	Control Center (<= v8.1)
Affected categorie(s)/product(s):	Fujitsu ETERNUS CS8000 (Control Center)
Remediated product version(s):	v8.1A SP02: P04, v8.0A SP01: P03 H035
Related Advisory/Bulletin(s)/Inform(s):	CVE ID requests pending at MITRE
Initial release / Last update:	June 1, 2022 / N/A
Reference(s) / Fujitsu PSIRT ID:	PSS-IS-2022-050316

Document Target Audience and Security Classification:

Target Audience: Customer & Service Partner & Fujitsu - Document Classification: Unclassified

PROBLEM / DESCRIPTION

In May 2022, the Fujitsu PSIRT received intelligence on two vulnerabilities present in **Fujitsu ETERNUS CS8000 (Control Center)**.

These vulnerabilities reside in two separate components of the Control Center software, accessible by users on the network, which pass user input directly to privileged "shell_exec" and "system" functions via files grel.php and w_view.php core files. An attacker is therefore able to influence parameters and inject special characters to execute arbitrary commands on the system.

The Fujitsu PSIRT has no knowledge of working code, able to potentially exploit these vulnerabilities, at the time of publication.

SITUATION

The U.S. MITRE and NIST ITL were requested by the Fujitsu PSIRT for publication of dedicated CVE IDs on these vulnerabilities, while for each assigning a suggested CVSSv3 base score of Critical (9.8).

The Fujitsu PSIRT has estimated a Fujitsu ARF (Affection Risk Factor), based on the component prevalence, component security record, and component fix/mitigation expenditure. The currently estimated Fujitsu ARF is Low-Medium (2).

SOLUTION / REMEDIATION

Based on the intelligence information available, the Fujitsu PSIRT rated the vulnerabilities, as a low-medium-level threat to the Fujitsu product portfolio, due to the low prevalence and limited exploitability of other similar components in Fujitsu products.

Relevant Fujitsu PSIRT members and adjacent development and engineering departments were already informed.

The Fujitsu PSIRT requested a mitigation of the underlying vulnerabilities, via software package updates, and has also provided further instructions on the remediation. Fujitsu product updates were made available consecutively, while all intelligence provided by the Fujitsu PSIRT is processed continuously.

An update for Fujitsu ETERNUS CS8000 (Control Center) is available with versions v8.1A SP02 P04 and v8.0A SP01 P03 H035 (remediated product versions) respectively*.

*A dedicated customer request to Fujitsu via ServiceNow or Support Assistant is required, due to the software distribution model.

ADDITIONAL INFORMATION

At this point Fujitsu PSIRT issue PSS-IS-2022-050316, addressing these vulnerabilities, is in MITIGATED/RESOLVED state, but will be updated as necessary, in the Fujitsu PSIRT PRODUCT SECURITY section of the Fujitsu Product Support website.

Fujitsu products / components not listed in this document are not affected.

There are currently no further recommendations by the Fujitsu PSIRT on workarounds, with regards to the vulnerabilities. Instead, the Fujitsu PSIRT recommends customers to install the available Fujitsu product updates and follow general security best practices.

PUBLISHED BY THE FUJITSU PSIRT

Fujitsu Europe
The Fujitsu PSIRT (Product Security Incident Response Team)
E-mail: Fujitsu-PSIRT@ts.fujitsu.com
Internet: https://security.ts.fujitsu.com

Fujitsu Technical Support Pages: https://support.ts.fujitsu.com

