Fujitsu PSIRT — Security Notice

FUJITSU SOFTWARE INFRASTRUCTURE MANAGER (ISM) VULNERABILITY

ISS-IS-2023-071410

Affected component(s):	Fujitsu Software Infrastructure Manager (ISM) ismsnap
Affected category(s)/product(s):	Fujitsu Software Infrastructure Manager (ISM) (v2.8.0.060)
Remediated product version(s):	V2.8.0.061
Related Advisory/Bulletin(s)/Inform(s):	CVE-2023-39903
Original release / Last update:	July 31, 2023 / September 4, 2023
Reference(s) / Fujitsu PSIRT ID:	ISS-IS-2023-071410

PROBLEM / DESCRIPTION

In Jul. 2023, the Fujitsu PSIRT received internal intelligence on a vulnerability, present in **Fujitsu Software Infrastructure Manager (ISM)**.

That vulnerability resides in component "ismsnap" (in this specific case at: /var/log/fujitsu/ServerViewSuite/ism/FirmwareManagement/FirmwareManagement.log) of the ISM software, used for the collection of maintenance data. The vulnerability allows for the insecure collection and storage of authorization credentials in clear-text. Such credentials may include:

- User credentials (passwords), when performing any ISM "Firmware Repository Address" setup test ("Test the Connection").
- User credentials (passwords), when performing regular authorizations against an already configured remote firmware repository site, as set up in ISM "Firmware Repository Address".

A privileged attacker is therefore able to potentially gather such "ismsnap" maintenance data, either regularly as a trusted party allowed to export "ismsnap" data from ISM, or e.g. in case of compromise of the collecting agent / ISM management terminal, primarily if that maintenance data can be viewed by a principal / authority other than ISM Admin. The preconditions for an ISM installation to be generally vulnerable are:

- The "Download Firmware (Firmware Repository Server)" function must be enabled and configured.
- The character "\" (backslash) must be used as user credential (i.e. user/ID or password) of the remote proxy host / firmware repository server.

Note: "ismsnap" data additionally resides in ISM's internal "ismsnap" archive (DB) and local file system. However, access to these locations requires elevated privileges on the ISM appliance / system.

The Fujitsu PSIRT has no knowledge of working code or active campaign, able to potentially exploit this vulnerability, at the time of publication.

SITUATION

Based on the intelligence information available, the Fujitsu PSIRT rated the vulnerability in summary, as a medium-level threat to the Fujitsu product portfolio, due to the medium criticality, medium risk factor, and estimated low-medium exploitability.

The U.S. MITRE and NIST ITL was requested by the Fujitsu PSIRT for publication of dedicated CVE ID CVE-2023-39903 on this vulnerability. The estimated CVSSv3 base score is Medium (5.9).

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 Medium (3).

SOLUTION / REMEDIATION

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

The Fujitsu PSIRT requested a mitigation of the underlying vulnerability, via software package update, and has also provided further, internal recommendations on the remediation. Fujitsu product updates were already made available.

A final update for the Fujitsu Software Infrastructure Manager (ISM) is available:
https://security.ts.fujitsu.com/IndexDownload.asp?SoftwareGuid=D6CC3F50-7147-49F6-9A1F-1A81F3571BF0

ADDITIONAL INFORMATION

At this point Fujitsu PSIRT issue ISS-IS-2023-071410, addressing that vulnerability, is MITIGATED/RESOLVED, but may be updated as necessary, in the Fujitsu PSIRT PRODUCT SECURITY section of the Fujitsu Product Support website.

A brief ACL (List of Affected Fujitsu Categories & Products) follows below. Products not listed are either not affected or not supported. The following content is final.

Server (SRV)

AFFECTED SYSTEM	AFFECTION STATE	NEW FIXED VERSION	RELEASE DATE
Fujitsu ISM [for PRIMERGY, PRIMEQUEST]	AFFECTED	v2.8.0.061	AVAILABLE

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

RECOMMENDATION

The Fujitsu PSIRT recommends customers to install the available Fujitsu product updates and follow general security best practices.

Additionally, the Fujitsu PSIRT recommends to do the following:

- **ASSESSMENT:** Users are strongly recommended to determine if a customer environment is at risk, due to previous execution of "ismsnap" and its collected maintenance data being accessible by a principal / authority other than ISM Admin.
- **MITIGATION:** Users are strongly recommended to delete such collected maintenance data via the ISM management terminal, especially if such data is accessible by a principal / authority other than ISM Admin, to prevent any potential future abuse of such authorization credentials present in clear-text.
- **MITIGATION:** Users are recommended to immediately change any passwords used in context of the ISM "Firmware Repository Address" setup, in case such collected maintenance data was accessible by a principal / authority other than ISM Admin, and such users may have undesirably accessed "ismsnap" data.
- **PREVENTION:** Users are recommended to employ character "@" instead of "\" (backslash) for user credential (i.e. user/ID) of the remote proxy host / firmware repository server, e.g. "user@domain".
- **ADVANCEMENT:** With the aid of the Fujitsu PSIRT, the Fujitsu development has identified further minor issues in SNMPv3 configuration and automatic log transfer, where ISM-internal log data could potentially contain clear-text credentials. However, these are protected by the ISM administrative principal and cannot be exported from ISM. Fujitsu has plans to mitigate these low criticality issues with ISM v2.9.0 in Sep. 2023.

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

