Fujitsu PSIRT — Security Notice

FUJITSU FLASH BIOS UPDATE (DFI), ADMIN PACKAGE (CFF) VULNERABILITIES

PSS-IS-2022-061319

Affected component(s):	Flash BIOS Update (DFI), Admin Package (CFF) (Gen. 6)
Affected category(s)/product(s):	Fujitsu CELSIUS, ESPRIMO, FUTRO, LIFEBOOK, STYLISTIC
Remediated product version(s):	Fujitsu Flash BIOS Update (DFI), Admin Package (CFF) (Gen. 6) FIX/patch
Related Advisory/Bulletin(s)/Inform(s):	N/A
Original release / Last update:	August 15, 2022 / May 17, 2023
Reference(s) / Fujitsu PSIRT ID:	PSS-IS-2022-061319

PROBLEM / DESCRIPTION

In June 2022, the Fujitsu PSIRT received intelligence, by security researcher Stefan Kanthak, on vulnerabilities present in **Flash BIOS Update (DFI)** and **Admin Package (CFF)** (6th generation).

These reside in two separate components of the Flash BIOS Update (DFI) and Admin Package (CFF) software, downloadable by customers on the Fujitsu (EMEA) Product Support website. The components are subject to CAPEC-471 (Search Order Hijacking) and CWE-427 (Uncontrolled Search Path Element) weaknesses, which allow an attacker to induce the load of a rogue program from a foreign path, potentially with elevated privileges on the system due to the nature of the Fujitsu Flash BIOS Update (DFI) and Admin Package (CFF) software.

The Fujitsu PSIRT has knowledge of a working PoC (Proof of Concept) method, able to exploit these vulnerabilities, at the time of publication.

SITUATION

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

The U.S. MITRE and NIST ITL were not requested by the Fujitsu PSIRT for publication of dedicated CVE IDs on these vulnerabilities. The estimated CVSSv3 base score is High (7.3).

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 weaknesses, via software package updates, and has also provided further, internal instructions on the remediation. Fujitsu product updates will be made available consecutively, while all intelligence provided by the Fujitsu PSIRT is processed continuously.

A final update for the Fujitsu Flash BIOS Update (DFI) and Admin Package (CFF) (6th generation) software will be available as per the listing in this document.

ADDITIONAL INFORMATION

At this point Fujitsu PSIRT issue PSS-IS-2022-061319, addressing these vulnerabilities, is MITIGATED/RESOLVED, and documented 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 products will not receive any DFI/CFF update, and were labeled accordingly.

ESPRIMO D956, ESPRIMO D956/LL, ESPRIMO P556, ESPRIMO Q956, CELSIUS W570 (Power), ESPRIMO D957, ESPRIMO K557/20 (/24), CELSIUS R970 (Power), CELSIUS H770, CELSIUS H970, LIFEBOOK E547/E557 (vPro), LIFEBOOK P727, LIFEBOOK T937, LIFEBOOK U937, STYLISTIC R727, STYLISTIC R727 vPro, STYLISTIC V727, LIFEBOOK S937, CELSIUS H760, LIFEBOOK S936, LIFEBOOK U938, LIFEBOOK P728, LIFEBOOK S938, LIFEBOOK T938 (US), STYLISTIC Q738 (US), STYLISTIC Q509 (US), CELSIUS H980 (ODM), LIFEBOOK U939X (US), LIFEBOOK U729X (US), LIFEBOOK T939 (US), LIFEBOOK U939 (US), STYLISTIC Q739 (US)

The following affection states and DFI/CFF release dates for supported products are final.

Desktop PC (ESPRIMO)

AFFECTED SYSTEM	AFFECTION STATE	NEW FIXED VERSION	RELEASE DATE
Fujitsu ESPRIMO D556/2	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO D757	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO P556/2	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO P557 (Power)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO P757	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO P957 (Power)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO Q556/2 (/D)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu ESPRIMO Q957 (/MRE)	AFFECTED	LATEST	UPDATE AVAILABLE

Workstation (CELSIUS)

AFFECTED SYSTEM	AFFECTION STATE	NEW FIXED VERSION	RELEASE DATE
Fujitsu CELSIUS J550/2 (-L)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu CELSIUS M7010	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu CELSIUS M7010X	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu CELSIUS C780	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu CELSIUS R970B (Power)	AFFECTED	LATEST	UPDATE AVAILABLE

Thin Client (FUTRO)

AFFECTED SYSTEM	AFFECTION STATE	NEW FIXED VERSION	RELEASE DATE
Fujitsu FUTRO S540	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu FUTRO S740	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu FUTRO S940	AFFECTED	LATEST	UPDATE AVAILABLE

Mobile (CELSIUS/LIFEBOOK/STYLISTIC)

AFFECTED SYSTEM	AFFECTION STATE	NEW FIXED VERSION	RELEASE DATE
Fujitsu CELSIUS H780 (ODM)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu CELSIUS H7510 (ODM)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK E547/E557 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U727 (6th Gen)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U747/U757	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U747/U757 (6. Gen)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK E448/E458	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK E449/E459	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK E548/E558 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U728 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U748/U758 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK A359 (ODM)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK A3510 (ODM)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK E549/E559 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U729 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U749/U759 (US)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK E5410/E5510	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U7310	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U7410/U7510	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U9310 (R/B)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu LIFEBOOK U9310X (R/B)	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu STYLISTIC Q5010	AFFECTED	LATEST	UPDATE AVAILABLE
Fujitsu STYLISTIC Q7310	AFFECTED	LATEST	UPDATE AVAILABLE

Other **CCD platforms**, such as Tiger Lake, Jasper Lake and Alder Lake, as well as **Server products** (PRIMERGY and PRIMEQUEST), **Storage products** (ETERNUS) and **Server BS2000 products** (SE, AU) are NOT AFFECTED by any of the vulnerabilities.

RECOMMENDATION

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

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

