SERVICE FACTS on SECURITY NOTICE

APACHE LOG4J VULNERABILITY
("LOG4SHELL")
(PSS-IS-2021-121000)

**AFFECTED COMPONENT(S):**
Apache log4j (v2.0-alpha1 – v2.12.3 and v2.13.0 – v2.17.0)

**AFFECTED CATEGORY(S)/PRODUCT(S):**
Fujitsu Software ServerView® Suite (SVS), Fujitsu SecDocs

**REMEDIATED PRODUCT VERSION(S):**
Fujitsu SVOM (Linux) FIX/patch

**RELATED ADVISORY/BULLETIN(S)/INFORM(S):**
BSI-CB-K21-1264, CERT-VU-930724

**INITIAL RELEASE / LAST UPDATE:**
December 10, 2021 / February 24, 2022

**REFERENCE(S) / FUJITSU PSIRT ID:**
PSS-IS-2021-121000

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

**PROBLEM / DESCRIPTION**

In December 2021, the Fujitsu PSIRT received open-source intelligence on a new threat referred to as *Log4Shell*.

Log4Shell is an RCE (Remote Code Execution) 0-day exploit, found in multiple log4j logging software versions. That exploit allows to mount successful and effective attacks against victims running named Java logging library. According to the researchers, the impact of the exploit is to gain full system control. Besides the Log4Shell vulnerabilities, this document addresses further vulnerabilities found in Apache log4j.

The Fujitsu PSIRT has knowledge of working code, able to potentially employ Log4Shell, not requiring any elevated or otherwise special permissions on a given victim system, except for remote connectivity.

**SITUATION**

The U.S. NIST ITL and other bodies have already reported on Log4Shell (CVE-2021-44228 and CVE-2021-45046), while assigning a max. CVSSv3 base score of Critical (10.0).

Although CVE-2021-45105, CVE-2021-44832 and legacy CVE-2017-5645 on log4j version 2.x are not part of Log4Shell, these vulnerabilities are considered as well. Also, CVE-2021-4104 and CVE-2019-17571 on log4j version 1.x are considered, mitigations/fixes applied, and further software updates provided for:

- Brocade SANnav for Fujitsu ETERNUS SF by mid-January 2022.
- Fujitsu FlexFrame by the end of January 2022.
- Most Fujitsu Software ServerView® Suite (SVS) components: t.b.d. / date under review.
- Fujitsu Software Infrastructure Manager (ISM) by the end of April 2022.
- Fujitsu openUTM (+WebAdmin) by mid-2022 and BeanConnect by end of 2022.
- Fujitsu ETERNUS SF (+MA) at a date yet to be announced.

The Fujitsu PSIRT has estimated a Fujitsu ARF (Affection Risk Factor), based on log4j prevalence, log4j security record, and log4j fix/mitigation expenditure. The currently estimated Fujitsu ARF is Medium-High (4).

**SOLUTION / REMEDIATION**

Based on the intelligence information available, the Fujitsu PSIRT rated the Log4Shell exploit, and the associated conglomerate of log4j vulnerabilities, as a medium-high-level threat to the Fujitsu product portfolio, due to the prevalence but still limited exploitability of corresponding vulnerable log4j packages in Fujitsu products.

Due to the nature of the Log4Shell exploit, the Fujitsu PSIRT already notified all Fujitsu PSIRT members, as well as adjacent development and engineering departments.

The Fujitsu PSIRT requested a fix of the underlying vulnerabilities, via software package updates, and has also provided further instructions on immediate log4j vulnerability mitigation. Fujitsu product updates are made available consecutively, while all intelligence provided by the Fujitsu PSIRT is processed continuously.

**ADDITIONAL INFORMATION**

At this point Fujitsu PSIRT issue PSS-IS-2021-121000, addressing the Log4Shell exploit and corresponding log4j vulnerabilities, is SEMI-MITIGATED/RESOLVED, but will still be updated in regular intervals, in the Fujitsu PSIRT PRODUCT SECURITY section of the Fujitsu Product Support website.

A brief ACL (List of Affected Fujitsu Categories & Products) follows below. Software not listed is either not affected, or has not been actively requested by customers for listing despite being unaffected. The following content is subject to change, while the Fujitsu PSIRT gathers new intelligence on overall Fujitsu product affection.

**Client Computing Devices (CCD)**
- eLux RP on FUTRO: NOT AFFECTED (log4j not present)
- INTELLIEGDLE A/G: NOT AFFECTED (log4j not present)
- Workplace Protect: NOT AFFECTED (log4j not present)

Further CCD products and components are not affected or not supported.

Fujitsu customers employing Fujitsu CELVIN should review QNAP QSA-21-58.

**Server (SRV)**
- BX400/BX900 MMB: NOT AFFECTED (log4j not present)
- SBAX2, SBAX3: NOT AFFECTED (log4j not present)
- SB6, SB11, SB11a: NOT AFFECTED (log4j not present)
- iRMC on PRIMERGY: NOT AFFECTED (log4j not present)
Further SOL products and components are not affected or not supported.
Fujitsu customers employing Marvell QCC GUI should migrate to Windows Admin Center, PowerKit, or QCC CLI.

### Storage (STR)

- ETERNUS AB/HB: NOT AFFECTED
- ETERNUS CS800: NOT AFFECTED
- ETERNUS CS8000: NOT AFFECTED
- ETERNUS DX/AF: NOT AFFECTED
- ETERNUS JX: NOT AFFECTED
- ETERNUS SF: NOT AFFECTED
- ETERNUS SF MA: NOT AFFECTED
- ETERNUS LT20/40/60 NOT AFFECTED
- ETERNUS LT140/260 NOT AFFECTED

Further STR products and components are not affected or not supported.
Fujitsu customers employing Brocade SANnav should review Broadcom BSA-2021-1651.

### Solutions (SOL)

- FlexFrame: NOT AFFECTED
- NECOP: NOT AFFECTED
- PRIMEFLEX for MS S2D NOT AFFECTED
- PRIMEFLEX for SAP HANA NOT AFFECTED

Further SOL products and components are affected indirectly (NECoP, PRIMEFLEX).
Fujitsu customers with Nutanix and VMware support contracts should request updates from these vendors.

### Enterprise Platform Services (EPS)

- BS2000 Hardware: NOT AFFECTED
- BS2000 Software: NOT AFFECTED
- openSEAS:
  - openFT: NOT AFFECTED
  - openUTM: NOT AFFECTED
  - openUTM (WebAdm.): NOT AFFECTED

Fujitsu customers with support contracts with ISM or VMware should request updates from these vendors.
BeanConnect: NOT AFFECTED (log4j v1.2 present in BC, JMSAppender + SocketServer class not used)
WebTransactions: NOT AFFECTED
- SecDocs: AFFECTED (log4j v2.11 present in SecDocs) MITIGATION AVAILABLE

Further EPS products and components are not affected.

Global Technical Support (GTS)
- Fujitsu AIS Connect: NOT AFFECTED (log4j not present)
- PTC Axeda (AIS Con.): NOT AFFECTED (log4j not present)

Further GTS products and components are not affected or not supported.

Other applications, such as Fujitsu ScanAllPro, ScanSnap Home, ScanSnap Manager, ScanSnap Organizer and CardMinder are NOT AFFECTED by any of the log4j vulnerabilities.

There are currently no further recommendations by the Fujitsu PSIRT on mitigations or workarounds, with regards to the log4j vulnerabilities. The Fujitsu PSIRT asks customers to install Fujitsu product updates and follow general security best practices, e.g. as issued by national CERTs, ENISA and CISA.

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

All rights reserved, including intellectual property rights. Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner. For further information see ts.fujitsu.com/terms_of_use.html