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 categorie(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 / January 12, 2022
Reference(s) / Fujitsu PSIRT ID:	PSS-IS-2021-121000

Document Target Audience and Security Classification:

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 a 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 as necessary.

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 continously.

An emergency update for the Fujitsu Software ServerView® Suite (SVS) Operations Manager (SVOM) is available:
https://support.ts.fujitsu.com/IndexDownload.asp?SoftwareGuid=b2d7207f-bdd3-4f9b-aa7c-4372d414ab99
https://support.ts.fujitsu.com/IndexDownload.asp?SoftwareGuid=a3e6bb34-a56f-4d7c-a3c2-ec02e8e7490e

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)

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

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)
- ISM for PRIMERGY, PQ: NOT AFFECTED (log4j v1.2 present in ISM core, JMSAppender not used, SocketServer class not used)
- PQ unified firmware:
  Mgmt. Board Web UI: NOT AFFECTED (log4j not present)
- PrimeUp NOT AFFECTED (log4j not present)
- ServerView VIOM: NOT AFFECTED (log4j v1.2 present in SVVIOM, JMSAppender + SocketServer class not used)
- ServerView IM: NOT AFFECTED (log4j v1.2 present in SVIM, JMSAppender + SocketServer class not used)
- ServerView OM: AFFECTED (log4j v2.12 present in SVOM) MITIGATION AVAILABLE
- ServerView OM/UM: NOT AFFECTED (log4j v1.2 present in OM/UM, JMSAppender + SocketServer class not used)
- ServerView Rem. Con. NOT AFFECTED (log4j not present)
- ServerView RAID NOT AFFECTED (log4j not present)

- SVS Services for ISM: NOT AFFECTED (log4j v1.2 present in SVSSISM, JMSAppender + SocketServer class not used)
- SVS UME +LinuxLife: NOT AFFECTED (log4j v1.2 present in BCM OCM, JMSAppender + SocketServer class not used)
- SVS VMware vCenter: NOT AFFECTED (log4j v1.2 present in SVVMvC, JMSAppender + SocketServer class not used)
- SVS VMware Op. Mgr.: NOT AFFECTED (log4j v1.2 present in SVVMOM, JMSAppender + SocketServer class not used)
- SOA SysRollout Service: NOT AFFECTED (log4j v1.2 present in SOASRS, JMSAppender + SocketServer class not used)
- SOA Pro. Mgmt. Service: NOT AFFECTED (log4j v1.2 present in SOAPMS, JMSAppender + SocketServer class not used)

Further SRV 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 (log4j not present)
- ETERNUS CS800: NOT AFFECTED (log4j v1.2 present in CS800, JMSAppender + SocketServer class not used)
- ETERNUS CS8000: NOT AFFECTED (log4j v1.2 present in CentricStor, JMSAppender + SocketServer class not used)
- ETERNUS DX/AF: NOT AFFECTED (log4j not present)
- ETERNUS JX: NOT AFFECTED (log4j not present)
- ETERNUS SF: NOT AFFECTED (log4j v1.2 present in ETERNUS SF, JMSAppender + SocketServer class not used)
- ETERNUS SF MA: NOT AFFECTED (log4j v1.2 present in ETERNUS SF MA, JMSAppender + SocketServer class not used)
- ETERNUS LT20/40/60 NOT AFFECTED (log4j not present)
- ETERNUS LT140/260 NOT AFFECTED (log4j not present)

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 (log4j v1.2 present in FF, JMSAppender + SocketServer class not used)
- NECoP: NOT AFFECTED (log4j not present in NECoP ex factory / as delivered by Fujitsu)
- PRIMEFLEX for MS S2D NOT AFFECTED (log4j not present)
- PRIMEFLEX for SAP HANA NOT AFFECTED (log4j not present)

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 (log4j v1.2 present in WA, JMSAppender + SocketServer class not used)
  - 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

