Security Bulletin:

Log4Shell – Unauthenticated RCE 0-day exploit

Author : Atos BDS TI Team
Created : 2021-12-13
Last Update : 2022-05-30
Revision : 2.0
Keywords :

TLP:WHITE

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Executive summary

A vulnerability is present in all applications embedding Log4j (ver. 2.0 to 2.14.1.) for audit logging feature. Mainly Apache stack but also applications like Elastic search, Redis, etc. The vulnerability is based on forcing applications to log a specific string which forces vulnerable system to download and run malicious script from attacker-controlled domain. According to security researchers, apps and services across the globe has already been actively scanned for vulnerable versions of Log4j by malicious actors. Some Atos products may propose the vulnerable component in their delivered distribution.

Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
CVE-2021-44228	10	CWE-502 Deserialization of Untrusted Data CWE-20 Improper Input Validation CWE-400 Uncontrolled Resource Consumption

Affected products

The vulnerability affects all products that use these specific log4j versions independently from software or operating system within which it is used. Vulnerability exists in log4j library not in Operation Systems or Vendor software itself.

Atos Product line	Version	Status	Comments
Bull Sequana Edge series		Not affected	The Bull Sequana Edge servers do not make use of the vulnerable library.
Bull Sequana S series		Not affected	The Bull Sequana S servers do not make use of the vulnerable library.
Bull Sequana XH series		Not affected	The Bull Sequana XH servers are not affected by themselves, but they may come with delivered environment for HPC which may include a vulnerable Log4j component (e.g. ElasticSearch). However, it is not susceptible to be impacted due to usage of the Java Security Manager.
All IDnomic products		Not affected	Those products do not embed the vulnerable component.

Although ATOS makes effort to provide accurate and complete information, ATOS shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

Recommendations

To detect if the log4j library is present on a linux machine please execute the following commands:

```
find / -iname "*log4j*" -print

lsof | grep log4j
```

Available Vendor Patches

Atos has not yet provided a patch for its

Available Workarounds

Start your Java Virtual Machine (JVM) server with

```
log4j2.formatMsgNoLookups
```

set to true, by adding

```
"-Dlog4j2.formatMsgNoLookups=True"
```

To be applied everywhere.

Available Mitigations

Starting with version 2.15.0 of log4j, the default configuration sets `formaMsgNoLookups` to `True`.

For the exploitation of the vulnerability the targeted web server needs to have the capacity to connect to a rogue server. Isolated networks are likely protected.

Available Exploits/PoC

Exploitation in the wild of the vulnerability has been observed. The current exploits leverage some LDAP rogue servers.

Details

On Thursday December 9th, 2021, around 8 AM CET new remote code execution exploit vulnerability has been publicly disclosed by security researcher @P0rZ9 on Twitter. Discovered during a bug bounty engagement against Minecraft servers, the vulnerability is far more impactful than some might have expected. As described by the Recorded Future researchers “Log4j is included with almost all the enterprise products released by the Apache Software Foundation, such as Apache Struts, Apache Flink, Apache Druid, Apache Flume, Apache Solr, Apache Flink, Apache Kafka, Apache Dubbo, (...). also, in open-source projects like Redis, ElasticSearch, Elastic Logstash, the NSA’s Ghidra, and others”.

Described further Luna Sec researchers has tested and shared extensive report on this 0-day vulnerability on their blog. According to researchers exploit exist in popular Java login library log4j allowing unauthenticated threat actor to remotely execute code on victims’ machine by login certain

string. So far it has been determined that impact is wide and any application or service using JDK or JNDI via LDAP is potentially vulnerable.

Further details, including IoCs can be obtained from Atos Threat Intelligence report.

References

1. Atos Threat Intelligence Team, Log4Shell – Unauthenticated RCE 0-day exploit, Vulnerability Analysis
2. https://logging.apache.org/log4j/2.x/security.html
3. https://access.redhat.com/security/cve/cve-2021-44228

List of changes

Version	Date	Description
0.1	Dec. 13, 2021	Initial neutralization version
0.2	Dec. 15, 2021	Updated neutralization version with Bull Sequana S status. Relaxing TLP constraint.
2.0	May 30, 2022	First public version.

Glossary of terms

Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability.
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated. Security bulletins issued during this phase are numbered 0.x.
POC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression. Security bulletins issued during this phase are numbered 1.x when private. Publicly disclosed bulletins are numbered 2.x.
TI	Threat Intelligence
TLP	Traffic Light Protocol
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update.

About this document

ATOS continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the Traffic Light Protocol (TLP)[1] to bring attention of owners of the potentially affected ATOS products. ATOS recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although ATOS makes effort to provide accurate and complete information, ATOS shall not be liable for technical or editorial errors contained in this Bulletin. The information provides is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither ATOS nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Product and company names mentioned herein may be trademarks of their respective owners.

About Atos

Atos is a global leader in digital transformation with 107,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea), listed on Euronext Paris and included on the CAC 40 ESG and Next 20 Paris Stock Indexes.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

[1] https://www.cisa.gov/tlp