KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Remote Code Execution in Apache Log4j” (KSA-2021-6)

In December 2021, several security advisories regarding the logging utility Apache Log4j for Java-based applications were published. Various Java-based software products of different vendors rely on Apache Log4j. An attacker, who successfully exploits the vulnerabilities, can execute arbitrary code or trigger a denial-of-service condition on the affected system.

For the affected products and services, Krones rates the likelihood of being exploited as low. Therefore, no specific action is required.

Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

No.	Likelihood of exploitation[1]	Affected products or services	Default state and remediation
1	Low	PCS systems (BOTEC) (few BOTEC setups use VMware vCenter Server 6.x – 7.x for virtualization)	• By default, the affected setup isn’t exposed to the internet. • Keep the BOTEC network isolated. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.
2	Low	PCS systems (BOTEC) (using Schneider Electric APC UPS)	• By default, the affected setup isn’t exposed to the internet. • Keep the BOTEC network isolated. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.
3	Low	SitePilot virtualization cluster (few SitePilot setups use VMware vCenter Server 6.x – 7.x for virtualization)	• By default, the affected setup isn’t exposed to the internet. • Keep the SitePilot network isolated. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.
4	Low	SitePilot (using Schneider Electric APC UPS)	• By default, the affected setup isn’t exposed to the internet. • Keep the SitePilot network isolated. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

5	Low	Cisco firewalls with Firepower Threat Defense 6.x • Cisco Industrial Security Appliance 3000 • Cisco Firepower 2110 Security Appliance	• By default, the affected setup isn't exposed to the internet. • Keep the firewall setup isolated. • Krones updates affected Firepower firewalls individually (managed by Krones).
6	Very low (unpatched) None (patched on 2021-12-20)	ReadyKit	• By default, exploitation requires local access to the ReadyKit. Exploitation via networks isn't possible. • Krones updated all commissioned ReadyKits that were online on 2021-12-20. • Krones updates remaining ReadyKits during commissioning (managed by Krones).
7	None	DART with software version 3.x – 9.x.	• By default, exploitation isn't possible due to strict configuration. • No specific action required.
8	None	IRIS (using iPanel touch display, and APC620/APC810) based on Windows XP Embedded: • ENYA • FIONA • GLORIA	• By default, exploitation isn't possible due to strict configuration. • No specific action required.
9	None	System Logistics GmbH Warehouse Control System (WCS)	• By default, WCS doesn't use the Log4j utility for logging. • No specific action required.
10	None	SitePilot LD, SitePilot LM	• By default, exploitation isn't possible due to strict configuration. • No specific action required.
Krones may add additional affected products or services, or update remediations as soon as there is new information available.			

Workarounds and mitigations

The following specific workarounds and mitigations are recommended in addition to the remediation measures listed above to further reduce the risk originating from the security vulnerabilities:

- If applicable, use firewalls to limit outgoing network traffic to the internet.
- If applicable, monitor your complete network traffic to detect anomalous traffic to the internet.

Security contact

If you have any questions regarding this security advisory or other security-related questions, please contact the Product Security Incident Response Team (PSIRT) of Krones: cyber.security@krones.com

OpenPGP key for confidential messages:
https://www.krones.com/ext/securitytxt/cyber.security@krones.com.asc

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Appendix A: Technical description of the vulnerabilities

This section describes the vulnerabilities in detail. The CVSS v3 base scores are the current severity rating according to the original security advisories and do not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2021-44228

Apache Log4j from 2.0-beta9 to 2.14.1[2] does not protect against attacker-controlled JNDI endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from JNDI endpoints (like LDAP servers) when message lookup substitution is enabled.

The CVSS v3.0 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

Vulnerability CVE-2021-45046

Apache Log4j from 2.0-beta9 to 2.15.0[2] protects insufficiently against attacker-controlled Thread Context Map (MDC) input data if certain non-default configuration is present. An attacker who can craft malicious input data may execute arbitrary code.

The CVSS v3.0 base score for the vulnerability is 9.0 (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).

Vulnerability CVE-2021-45105

Apache Log4j from 2.0-alpha1 to 2.16.0[2] does not protect against uncontrolled recursion from self-referential lookups. An attacker who controls Thread Context Map data can cause a denial-of-service condition.

The CVSS v3.0 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Vulnerability CVE-2021-44832

Apache Log4j from 2.0-beta7 to 2.17.0[2] is vulnerable to remote code execution if an attacker can modify the Log4j configuration to use a JDBC Appender with a data source referencing a JNDI URI.

The CVSS v3.0 base score for the vulnerability is 6.6 (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).

Vulnerability CVE-2021-4104

Apache Log4j 1.2 is vulnerable to deserialization of untrusted data if 1) the JMSAppender is in use (non-default component) and 2) the attacker can provide certain non-default configurations. An attacker, who can control log messages or log message parameters, plus, is able to write configuration on the system, can execute arbitrary code similar to CVE-2021-44228.

The CVSS v3.1 base score for the vulnerability is 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

[2] Apache released numerous security releases for Java 6 and Java 7 that are also not affected. Please read the official release notes by the Apache Software Foundation.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Appendix B: Further information

- Original security advisories by the Apache Software Foundation - Log4j – Apache Log4j Security Vulnerabilities
- Information regarding security vulnerabilities in Apache Log4j 1.x - https://logging.apache.org/log4j/1.2/

Appendix C: Changelog

Version	Date	Changes
1.0	2021-12-14	Initial publication by the Krones PSIRT
1.1	2021-12-17	Updated information about SitePilot LD, SitePilot LM Added information about CVE-2021-45046, CVE-2021-4104
1.2	2021-12-20	Added Schneider Electric APC UPS (PCS systems, SitePilot) Updated information about ReadyKit Added information about CVE-2021-45105
1.3	2022-01-11	Added IRIS based on Windows XP Embedded Updated information about Cisco FTD and CVE identifiers Added information about CVE-2021-44832
1.4	2022-02-16	Updated remediation of affected products using VMware vCenter Server Linked dedicated website about security vulnerabilities in Apache Log4j 1.x
1.5	2022-06-10	Updated remediation of affected BOTEC using VMware vCenter Server