Eaton Security Bulletin

ETN-SB-2021-1006: Critical Vulnerabilities reported in Apache log4j – Impact to Eaton Products

Date	Overall Risk	CVSS v3.0
01-Apr-2024	Critical	10.0

Overview

Eaton Product Security Incident Response Team (PSIRT) has become aware of critical vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832) in Apache log4j. We are continuously evaluating the impact of these vulnerabilities to our products and are developing mitigation plans to address them.

By exploiting these vulnerabilities an attacker may be able to execute arbitrary code on the application server or create a Denial-of-Service condition (DOS) on the application. Arbitrary code can be executed by controlling log messages or log message parameters to run arbitrary code loaded from attacker-controlled servers when message lookup substitution is enabled. A DOS attack can be executed by crafting malicious input data that contains a recursive lookup, that could lead to process termination due to a Stack overflow error.

Impacted Eaton Product(s) & Version(s)

The following Eaton products directly or indirectly utilize Apache log4j and are impacted by these vulnerabilities:

- Yukon:
  - 7.1.x, 7.2.x, 7.3.x, 7.4.x, 7.5.x all versions
  - 9.0.x, 9.1.x all versions
- Network Manager
  - All versions 8.7.x and higher
- Visual Capacity Optimization Manager (VCOM)
  - All versions prior to version 6.7.0
- Visual Power Manager (VPM)
  - All versions prior to version 6.7.0
- Visual Data Center (VDC)
  - All versions prior to version 6.7.0
- Intelligent Power Manager (IPM)
  - All 2.x versions

- PAEM
  - All versions prior to version 1.0.3.12

Vulnerability Details

CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker-controlled LDAP and other JNDI related endpoints. Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

CVE-2021-45046: The fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. When the logging configuration uses a non-default Pattern Layout with a Context Lookup, attackers with control over Thread Context Map (MDC) input data can craft malicious input data using a JNDI Lookup pattern, resulting in an information leak and remote code execution in some environments and local code execution in all environments; remote code execution has been demonstrated on MacOS, Fedora, Arch Linux, and Alpine Linux.

CVE-2021-45105: The updated Log4J versions did not protect from uncontrolled recursion from self-referential lookups. When the logging configuration uses a non-default Pattern Layout with a Context Lookup, attackers can perform a DOS attack by crafting malicious input data that contains a recursive lookup, resulting in a StackOverflowError that will terminate the process.

CVE-2021-44832: Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2 by limiting JNDI data source names to the java protocol.

Internet facing systems are exposed to a greater risk.

Remediation & Mitigation

While Eaton is currently analyzing the impact of these reported vulnerabilities to our products and is preparing appropriate mitigation plans, we have already released configuration updates to the following products.

- **Yukon & Network Manager**
  - **Permanent Remediation**

    Yukon maintenance releases containing the permanent fix for the targeted Log4j CVE are now ready for versions 7.3.x, 7.4.x, 7.5.x, 9.0.x and 9.1.x. In the coming months, you will be contacted by a member of our customer support team, or by the Deployment Engineer assigned to your RF deployment project, to schedule this important maintenance upgrade. In the interim, ensure that you have performed the previously recommended mitigation steps that are also detailed in the “Interim Mitigation” section below.

    Important Remediation Note: Yukon v7.1.x and v7.2.x Users

Customers using Yukon v7.1.x and v7.2.x will be required to upgrade to a minimum version of Yukon v7.3 to apply the permanent fix to address the vulnerabilities. A minimum Operating System version of Server 2016 is required for Yukon v7.3. Eaton will assist in transitioning to Yukon 7.3 or higher. If you cannot upgrade to the required 7.3 version, you will need to rely on the interim mitigation steps until you can move versions.

- **Interim Mitigation**

A PowerShell script is available to download and run on your Yukon installation. Identify the installed version of Yukon by logging into the software, scrolling down to the bottom of the web page and viewing the "Yukon Version" in the copyright area of the webpage. For example:
Once the version has been identified, follow the remaining mitigation steps.

Available script files

- **Yukon v7.1 - v9.1**
  - https://eatonfilesharing.box.com/s/f5ilxbnspw8a4fr76rorftj0pj4qqj29
- **Network Manager v8.7.0 - v9.1.0**
  - https://eatonfilesharing.box.com/s/6r4wz9jr972hrs11jb18c961figt1bxj

Important Note: Yukon v7.1.x Users

For users of Yukon v7.1 users will no longer be able to use the Apps link on the bottom of the Yukon webpage to launch the Java clients including Database Editor and Commander. Despite this loss of functionality, we strongly recommend you perform this mitigation process to secure your server.

Applying the update to the Yukon software all versions

1. Using the link above, download the "yukon_scrub_log4j.zip" from Box.com.
2. Unzip the file which will contain "scrub_log4j.ps1" and "scrub_log4j.cmd."
3. Stop all Yukon services (including the EIM, if applicable).
4. Run the script "scrub_log4j.cmd". (Note the script will automatically create backups of the modified files saved in the original folders)
   a. \Yukon\Client\bin\log4j-core-*.jar.yyyymmdd-hhmmss.bak
   b. \Yukon\Client\bin\api.war.yyyymmdd-hhmmss.bak
   c. \Yukon\Server\web\webapps\ROOT\WEB-INF\lib\log4j-core-*.jar. yyyymmdd-hhmmss.bak
   d. \Yukon\Server\Extras\Enterprise Integration Module\api.war.bak
5. If the EIM is present, follow the instructions under the heading "Confirming the EIM was updated correctly" to verify it was updated correctly.

Applying the update to the Network Manager software all versions (if applicable)

1. Using the above link, download the "network_manager_log4j.zip" file from Box.com.
2. Unzip the file which will contain "log4j-core-2.13.1.jar."
3. Stop the Network Manager service.

4. Navigate to the "lib" directory within your Network Manager installation (for example: "C:\Program
5. Files\Yukon\Network Manager\nmee-8.7.0\lib").
6. Rename the existing “log4j-core-2.13.1.jar” to “log4j-core-2.13.1.backup.jar” as a backup.
7. Copy the downloaded “log4j-core-2.13.1.jar” into the "lib" directory.

Confirming the EIM was updated correctly (if applicable)

The provided scripts attempt to apply the mitigation to the Yukon EIM .war file. Because the EIM installation may not be in the default directory structure, it is necessary to manually check that the proper WAR file was updated. To confirm:

1. Navigate to the Tomcat configuration directory (for example C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf\Catalina\localhost).
2. Open the “api.xml” file and verify the location of the "docBase" field in this file.
    a. Example: <Context path="/api" docBase="C:\Yukon\Server\Extras\Enterprise Integration Module\api.war"/>
3. If the “docBase” parameter points to your Yukon installation structure and that folder shows an updated WAR file and the expected backup, the update is confirmed.
4. If the “docBase” parameter points to a different location, you must either copy the updated .war from the default Yukon folder to the location noted by the “docBase” parameter or you must update the “docBase” parameter in the “api.xml” file to point to the updated WAR file in your Yukon folder.

Final Step: Restart your application server for the mitigation steps to take effect.

**Note the above steps are highly recommended. However, if it is not possible to perform these steps in the short-term, ensure that all unsecured connections to the Yukon server from sources external to the utility’s secure network are blocked. This will decrease the risk of a possible attack vector until the recommended remediation steps can be completed.*

If your system is hosted by Eaton, the support and deployment teams have applied the configuration changes necessary to mitigate the issue.

- ## VCOM, VPM, VPM Essential, VDC, EagleEye

To mitigate Log4J Vulnerability CVE-2021-44228 for VCOM, VPM, VPM Essential, VDC, EagleEye Product Release prior to 6.7, please follow the instructions provided below. For product release 6.7 and beyond, this vulnerability does not exist, thus no mitigation procedure is required.

1. Download script patch, 211212_all_0.0.0_SCP001_acbe91a82e4da4fbbae804dd041e085b.sh,

from the link above https://vault.optimumpathinc.com/owncloud/s/5qYVZsuCs7nLVKv

2. SCP the above script patch file on to all of the product servers under the /tmp/ directory.
    a. Note that all application servers in a distributed environment must be patched for this vulnerability.
3. Login to each of the servers as root user and execute this command: bash /tmp/211212_all_0.0.0_SCP001_acbe91a82e4da4fbbae804dd041e085b.sh
    a. If multiple servers are deployed in your architecture, apply the patch in the order of Master-DB server, Master Server and then the Probe Servers
    b. DO NOT REBOOT each server when the patch is completed. Complete patching ALL application server prior to rebooting servers.
4. Wait for the above command to finish on the application servers.
5. Reboot the application servers. If multiple servers are deployed then reboot the servers in the same order they were patched.

- **IPM 2 update**

- Hyper V: https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/power-management-software-connectivity/eaton-intelligent-power-manager/software/ipm-version-2/eaton-ipm-hyper-v.zip
- VMware: https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/power-management-software-connectivity/eaton-intelligent-power-manager/software/ipm-version-2/eaton-ipm-vmware.zip
- VirtualBox: https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/power-management-software-connectivity/eaton-intelligent-power-manager/software/ipm-version-2/eaton-ipm-virtual-box.zip
- Va update: https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/power-management-software-connectivity/eaton-intelligent-power-manager/software/ipm-version-2/eaton-ipm-va-update.zip
- Va update 2.3.0-1: https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power-distribution/power-management-software-connectivity/eaton-intelligent-power-manager/software/ipm-version-2/eaton-ipm-va-update-2.3.0-1.zip

Additional Steps

Eaton is currently analyzing the spread & impact of this vulnerability to our products and is preparing appropriate mitigation plans. Eaton recommends that customers ensure that all untrusted connections to Eaton products from sources external to the customer's secure network are blocked. This will decrease the risk significantly. And follow cybersecurity best practices to further protect their devices, as outlined below. Additional information on remediation and mitigation will be released as it becomes available.

- **PowerAlert Element Manager (PAEM)**

To mitigate this issue, users are requested to upgrade to the latest version 1.0.4.1. The latest version of the PAEM tool can be downloaded using this link. The PowerAlert Element Manager product webpage can be found using this link.

General Security Best Practices

- Restrict exposure to external networks for all control system devices and/or systems and ensure that they are not directly accessible from the open Internet.
- Deploy control system networks and remote devices behind barrier devices (e.g. firewalls, data diodes) and isolate them from business networks.
- Remote access to control system networks should be made available on a strict need-to-use basis. Remote access should use secure methods, such as Virtual Private Networks (VPNs), updated to the most current version available.
- Regularly update/patch software/applications to latest versions available, as applicable.
- Enable audit logs on all devices and applications.
- Disable/deactivate unused communication channels, TCP/UDP ports and services (e.g., SNMP, FTP, BootP, DHCP, etc.) on networked devices.
- Create security zones for devices with common security requirements using barrier devices (e.g. firewalls, data diodes).
- Change default passwords following initial startup. Use complex secure passwords or passphrases.
- Perform regular security assessments and risk analysis of networked control systems.

Eaton's Cybersecurity commitment

At Eaton we are committed to provide secure and stable products. Eaton's approach to cybersecurity advances trusted environments in a hyperconnected world, by integrating cybersecurity at the foundation of innovation for its product development and design processes. We consider cybersecurity to be a foundational building block that is critical to the design, deployment, and operation of digital solutions in the industrial world. Our industry leading IEC and UL endorsements mean that our customers can be confident that products and solutions they buy from us meet the same level of standards recommended by two key standard organizations across the globe. Eaton has multiple products that meet UL 2900-1, IEC 62443-4-2 cybersecurity standard and our Product Development processes are certified to IEC 62443 4-1

Eaton now offers Cybersecurity Services

For more details on cybersecurity best practices and leverage Eaton's Cybersecurity as a Service, please consult the following –

- Eaton offers a suite of cybersecurity assessment and life-cycle management services to help identify vulnerabilities and secure your operational technology network. These services can help you complete the recommended remediation and mitigation actions and strengthen your overall network security.

More information about these services are available at www.eaton.com/cybersecurityservices. If you need immediate support, please call +1-800-498-2678 to connect with a representative.

- Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN)
- Cybersecurity Best Practices Checklist Reminder (WP910003EN)

Additional Support and Information

For additional information, including a list of vulnerabilities that have been reported on our products and how to address them, please visit our Cybersecurity web site www.eaton.com/cybersecurity, or contact us at PSIRT@eaton.com.

Legal Disclaimer:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. EATON, ITS AFFILIATES, SUBSIDIARIES, AND AUTHORIZED REPRESENTATIVES HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND/OR CONDITIONS OF SECURITY, COMPLETENESS, TIMELINESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. YOU ARE SOLELY RESPONSIBLE FOR REVIEWING THE USER MANUAL FOR YOUR DEVICES AND GAINING KNOWLEDGE ON CYBERSECURITY MEASURES. YOU SHOULD TAKE NECESSARY STEPS TO ENSURE THAT YOUR DEVICE OR SOFTWARE IS PROTECTED, INCLUDING CONTACTING AN EATON PROFESSIONAL. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS, SO THE ABOVE LIMITATIONS MAY NOT APPLY. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EATON OR ITS AFFILIATES, OFFICERS, DIRECTORS, AND/OR EMPLOYEES, BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, ACTUAL, LIQUIDATED, EXEMPLARY, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF EATON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. EATON RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND AT ITS SOLE DISCRETION.

About Eaton:

Eaton is a power management company. We provide energy-efficient solutions that help our customers effectively manage electrical, and mechanical power more efficiently, safely, and sustainably. Eaton is dedicated to improving the quality of life and the environment using power management technologies and services. Eaton has approximately 85,000 employees and sells products to customers in more than 175 countries.

Eaton Security Bulletin

Revision Control:

Date	Version	Notes
14-Dec-2021	v1.0	Initial notification on CVE-2021-44228
31-Jan-2022	v2.0	Updated Public notification
01-Apr-2024	v3.0	Updated notification to include PAEM product

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com