Apache Log4J Vulnerability

Overview

A zero-day vulnerability involving the Apache Log4j utility was publicly disclosed on December 9, 2021 as announced on the Apache GitHub. Log4j versions prior to 2.15.0 are vulnerable to an unauthenticated remote code execution. On 10DEC2021 CVE-2021-44228 was published.

Log4j is an open-source Java logging library that is incorporated in many enterprise applications, open-source software, and potentially as a dependency in many other services. An attacker who can generate or control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Immediately upon learning of this vulnerability, GE Gas Power Product Security initiated its Product Security Incident Response plans to identify and mitigate potential risks within its environment and within its products.

Affected Products and Solution

Based on our current assessment, the GE Gas Power products listed below contain or use the vulnerable libraries. Ongoing investigation continues with the GE Gas Power product family and further updates will be provided.

Product	Log4j impact	Remediation
OPM Performance Intelligence	Impacted	Vulnerability fixed. No user actions necessary.
OPM Production Planning	Impacted	Vulnerability fixed. No user actions necessary.
MyFleet	Impacted	Vulnerability fixed. No user actions necessary.
Baseline Security Center (BSC)	Impacted	GE Gas Power is still validating the workaround provided by FoxGuard in Technical Information Notice – M1221-S01.
Baseline Security Center (BSC) 2.0	Impacted	GE Gas Power has tested and validated the component of the BSC 2.0 that is impacted (McAfee SIEM 11.x). The update and instructions can be downloaded from here: https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0029420
Asset Performance Management (APM)	Impacted	GE Digital has fixed the log4j issue on the APM. Validation and test completed in development environment and the team is currently deploying the fixes in the production environment.
Control Server	Impacted	Please see vCenter. Control Server is not directly impacted. It is impacted through vCenter.
Tag Mapping Service	Impacted	Vulnerability fixed. No user actions necessary. Updated to log4j 2.16

vCenter	Impacted	GE Gas Power has tested and validated the update provided by Vmware. The update and instructions can be downloaded from here: https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0029417

Workarounds and Mitigations

GE Gas Power Product Security is working to identify mitigations to address the log4j vulnerability and we will continue to update as new information becomes available and validation is completed.

Recommendations

GE Gas Power Cybersecurity and Engineering teams will continue to investigate internally as well as monitor industry-based news for any changes or updates. To reduce the risk that vulnerabilities like this may represent to the controls network, we recommend the implementation of a good defense-in-depth strategy as detailed in our GEH 6839 Secure Deployment Guide.

Additional Information

This advisory will be updated as more information becomes available. All deployed GE Gas Power products are under active investigation to determine whether they are affected by CVE-2021-44228.

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are engineered with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.

Document History

Version	Release Date	Purpose
1.0	December 21st, 2021	Log4J Vulnerability Assessment and Potential Product Impact Security Advisory
2.0	January 10th, 2021	Update BSC, Control Center and vCenter Remediation
3.0	January 21st, 2022	Updated remediation with links
4.0	September 29th, 2022	Updated document classification details

Resources

CISA: Apache Log4j Vulnerability Guidance