Apache Log4j Vulnerability – Updated 12 p.m. EST, December 13, 2021

Posted on December 13, 2021 by carlagajdecki

As you may know, a vulnerability within the Apache Log4j tool was identified on Friday, December 10, 2021 – tracked as CVE-2021-44228. Log4j is a logging framework created by Apache and used widely across the internet. Many, many services are potentially vulnerable to this exploit.

Our Security, Engineering and DevOps teams, under the direction of our CSO, conducted a full impact assessment once the vulnerability was initially identified early Friday morning and found no evidence of successful exploitation. In addition, our internal Red Team completed a deep analysis of our code as well as testing.

N-able can confirm there are **no vulnerabilities in these products**, as they do not utilize a vulnerable version of Apache Log4j or they may not utilize Apache Log4j at all:

- *N-central
- Backup
- Mail Assure
- MSP Manager
- Passportal
- SpamExperts
- SSO
- Take Control

Other products:

- RMM:
  - We have evaluated risk within RMM and have deployed patches for any vulnerable components as of 4 p.m. EST on December 10, 2021.
- Risk Intelligence:
  - Running a vulnerable version of Apache log4j
  - We are actively working on a patch and will update when we have more information.

* It was initially believed that N-central may have utilized a vulnerable version of Apache Log4j. After further investigation, it was determined that **N-central was not vulnerable** because N-central only utilizes the Log4j-API component, and not the Log4j-core component. We apologize for any confusion.

Our teams have not found any active exploits of this vulnerability and are confident in the safe use of N-able products. This potential vulnerability remains a top priority for our Security, Engineering and DevOps teams. We continue to monitor for any developments with this evolving industry-wide risk and will re-evaluate for exposure as necessary.

We don't recommend taking any N-able services offline. Your N-central system is not vulnerable and our RMM platform was patched on December 10. Thank you for your continued patience and understanding.

Additional Links:

CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Huntress blog: https://www.huntress.com/blog/rapid-response-critical-rce-vulnerability-is-affecting-java?fbclid=IwAR3I_cGEQBoJrCuDeIzL4m_8I-uyzDePYPsFF0wiOcM7WIAeT35ahqw9gR8

This entry was posted in Backup & Recovery, Backup & Recovery service updates, Mail Assure, MSP Anywhere, MSP Mail, MSP Mail service updates, MSP Manager, MSP Remote Monitoring & Management, MSP Remote Monitoring & Management service updates, MSP Service Desk, MSP Service Desk service updates, N-central, Passportal, Risk Intelligence, Risk Intelligence service updates, Security Notices, Take Control. Bookmark the permalink.