JMSAppender Associated with Log4j Vulnerability (CVE-2021-4104)

Summary

JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

Advisory Details

Severity

8.1 High

Advisory ID

CVE-2021-4104

First Published

12/17/2021

Last Updated

12/17/2021

CVSS Score

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

SolarWinds products do not use JMSAppender, and are not known to be affected by the vulnerability identified in CVE-2021-4104.

For more information on this CVE and guidance to mitigate this vulnerability, please visit our security advisory for CVE-2021-44228.