Apache Log4j Critical Vulnerability (CVE-2021-44228)

https://campus.barracuda.com/doc/96024380/

Update December 20, 2021 - Protections against Log4j Vulnerabilities

Since the original release of this article, Barracuda Networks has released updates to the attack patterns that can handle the newer vulnerabilities that have been released. The three attackdefs are described in the table below with details on the actual pattern names.

Vulnerabilities	Pattern	AttackDef Version	Release Date	Notes
CVE-2021-44228	log4j-rce-vulnerability	1.208	13 December 2021	First release
Various evasions and new attacks	log4j-rce-vulnerability	1.210	17 December 2021	Updated to attacks that do not use the closing "}"
CVE-2021-45105, CVE-2021-45046	log4j-rce-colon-vuln-strict log4j-rce-substition-strict	1.211	18 December 2021	Recursion & {ctx:) and other evasions. For enabling OS-Command-Injection-Strict, see the section later in this article.

Protecting against Log4j with Barracuda WAF-as-a-Service

Protective configurations against Log4j for Barracuda WAF-as-a-Service are rolled out automatically to all applications. For CVE-2021-45105 and CVE-2021-45056, you are required to manually enable OS-Command-Injection-Strict if their applications require this setting. If you need help with enabling these patterns, contact https://www.barracuda.com/support/index.

If you find false positives due to these settings and need help tuning the configurations for Barracuda WAF-as-a-Service, contact Barracuda Networks Technical Support.

Update: December 16, 2021 - Pattern to detect new evasion that does not use the closing “}”

Barracuda Networks recently observed that attacks are possible without using the closing curly bracket in the requests. The existing patterns will not detect such attempts. Detecting such attempts requires an aggressive pattern that could cause false positives. This pattern will be published as an *attackdef* in the coming days, along with the updates for any new evasions.

You can obtain the updated pattern from Barracuda Networks Technical Support and apply it manually. Contact Barracuda Networks Technical Support for next steps.

You can see the Proof of Concept for exfiltrating data from Log4j 2.15.0 here: https://www.praetorian.com/blog/log4j-2-15-0-stills-allows-for-exfiltration-of-sensitive-data/

December 14, 2021

Log4j is a Java-based logging audit framework within Apache. In Apache Log4j versions 2.14.1 and earlier, 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. This vulnerability impacts default configurations of several Apache frameworks, including Apache Struts2, Apache Solr, Apache Druid, and Apache Flink, which are used by numerous organizations.

This vulnerability is triggered when a malicious actor sends a specific string to the Log4j software – a somewhat simple action. The popular usage of Log4j presents multiple attack vectors for malicious actors. Recently, Barracuda Networks has seen attackers increasingly obfuscate their reconnaissance and attempts to exploit this vulnerability.

CVSS: 10 - Critical

For details, refer to the CVE-2021-44228 update from the National Vulnerability Database at NIST: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Barracuda Networks Product Status

Barracuda WAF-as-a-Service does not use Log4j, so it is not affected by this vulnerability.

Attack Detection and Protection

Barracuda WAF-as-a-Service

Barracuda Networks has released new signatures to detect and block Log4j exploit attempts. These signatures have been updated to handle the latest evasions seen in the field as of December 13, 2021. These signatures and settings will block both GET and POST requests attempting this exploit.