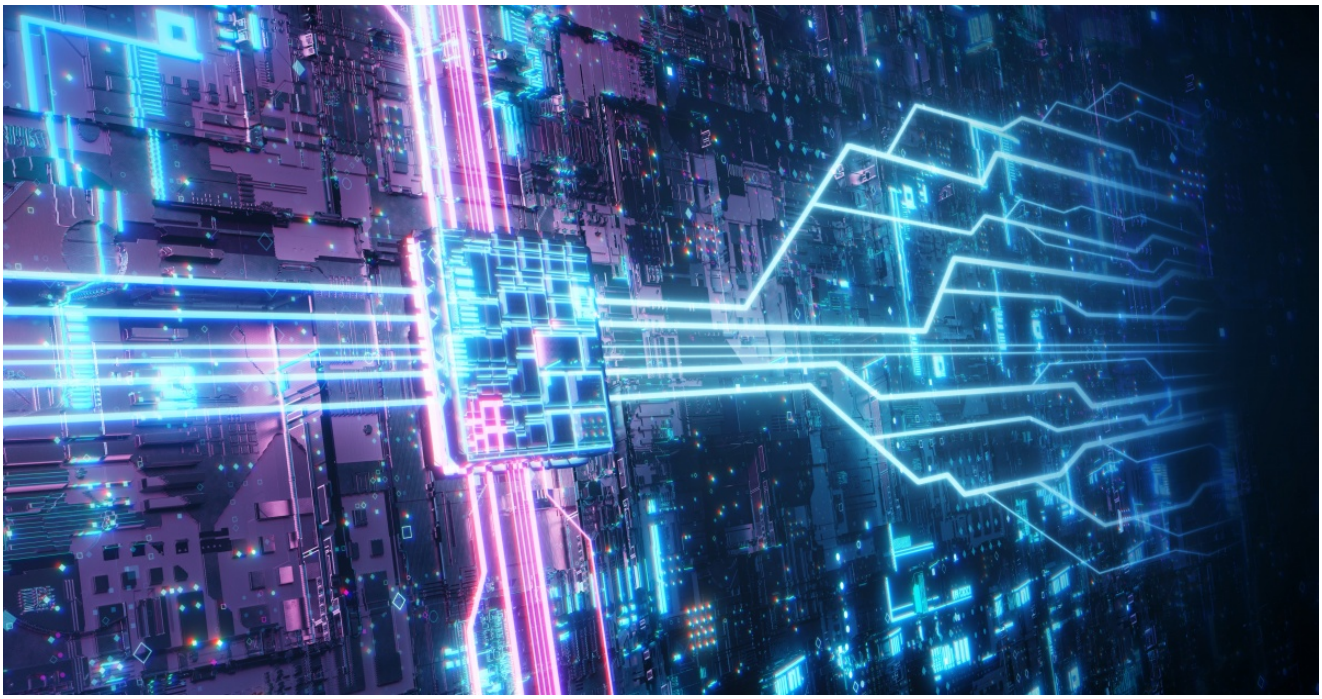
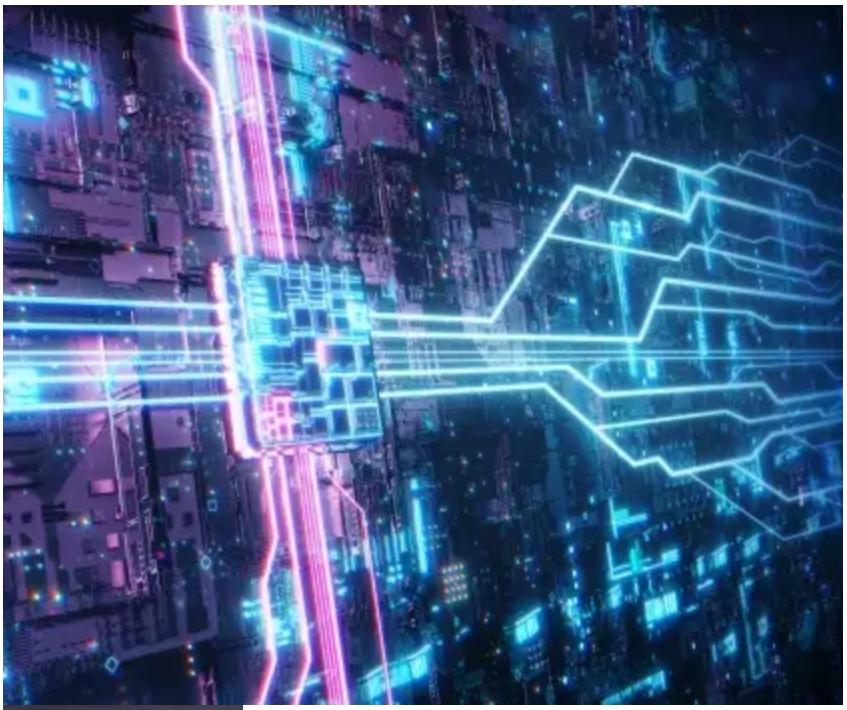
# Apache Log4j Zero-Day Being Exploited in the Wild

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apache-log4j-zero-day





Threat Hunter TeamSymantec

# Symantec products will protect against attempted exploits of critical CVE-2021-44228 vulnerability

**UPDATE December 20, 2021:** *The Apache Software Foundation has released a patch for a third vulnerability in Log4j. Version 2.17.0 of the software was released on December 17 after issues were discovered with the previous release (2.16). Apache said that 2.16 does not always protect from infinite recursion in lookup evaluation and is vulnerable to CVE-2021-45105, a denial of service vulnerability.*

**UPDATE December 15, 2021**: *Apache has patched a second vulnerability in Log4j. The vulnerability (CVE-2021-45046) arises from the fact that the fix for the previous vulnerability (CVE-2021-44228) did not completely prevent exploits in all circumstances.*

*According to Apache, the vulnerability occurs in certain non-default configurations. It could permit attackers to "craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack".*

A zero-day vulnerability (CVE-2021-44228) has been discovered in Apache Log4j which, if exploited, could permit a remote attacker to execute arbitrary code on vulnerable systems. Exploit code for this vulnerability, dubbed Log4Shell, has been shared publicly and multiple attackers are already attempting to exploit it.

**Q: Will Symantec protect against exploit attempts?**

**A:** Yes, Symantec products will guard against exploit attempts and payloads with the following detections:

**File-based**

- Trojan.Maljava
- CL.Suspexec!gen106
- CL.Suspexec!gen107
- CL.Suspexec!gen108
- Miner.XMRig!gen2
- Ransom.Khonsari
- Ransom.Tellyouthepass
- Ransom.Tellyouthepa!g1
- Ransom.Tellyouthepa!g2
- Linux.Kaiten
- Trojan Horse

**Machine learning-based**

Heur.AdvML.C

**Network-based**

- Attack: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j CVE-2021-45046
- Attack: Malicious LDAP Response
- Audit: Log4j2 RCE CVE-2021-44228
- Audit: Malicious LDAP Response
- Audit: Suspicious Java Class File Executing Arbitrary Commands

**Email-based**

Coverage is in place for Symantec's email security products

**Symantec Data Center Security** provides a range of protection for server workloads against this vulnerability:

- Prevention policies prevent malware from being dropped or executed on the system
- Ability to block or limit LDAP, http, and other traffic from server workloads and containerized applications using Log4j to internal trusted servers
- Prevention policies sandboxing provides protection from remote code execution by preventing execution of dual use tools, credential theft, and protecting critical system files and resources

**Web-based**

WebPulse observed traffic is currently protected for the Log4jShell vulnerability through normal processes

**Q: What is the significance of this vulnerability?**

**A:** Apache Log4j is a java-based logging utility. It is widely used in cloud and enterprise software services. The fact that an exploit was discovered prior to the creation of a patch only heightens the severity of the threat.

**Q: Has the vulnerability been patched?**

**A:** Yes, users are advised to update to version 2.15.0 immediately. Apache has also provided mitigation advice for users of earlier versions.

**Q: Is this vulnerability being exploited in the wild?**

**A:** Yes. Exploit code is publicly available and there are multiple reports of exploit attempts. To date, activity appears to be mainly centered on coin mining botnets but it is only a matter of time before attackers of all types attempt to leverage this exploit.

## Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

## Learn More Now

1. Broadcom Response to Log4j Vulnerability

2. Symantec Security Advisory

## About the Author

### Threat Hunter Team

#### Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

## Want to comment on this post?