Log4J Vulnerabilities - Sophos Resolutions (Updated to 10 Dec 2021)

The information provided below is referred from https://www.sophos.com/en-us/security-advisories/sophos-sa-20211210-log4j-rce.

- **CVE Number**

  2021-44228
  2021-45046

- **Discovery Date**

  Dec 10, 2021

- **Threat Level**

Critical

- **Response to Log4j**

On Thursday December 9, 2021, a severe remote code vulnerability was revealed in Apache's Log4J , a very common logging system used by developers of web and server applications based on Java and other programming languages. The vulnerability affects a broad range of services and applications on servers, making it extremely dangerous—and the latest updates for those server applications urgent. Sophos has observed widespread malicious attempts to exploit internet facing services using this vulnerability.

The customers can take to mitigate the vulnerability, the best fix is to upgrade to the patched version, already released by Apache in Log4j 2.16.0 to resolve the CVE-45056.

- **Affected Sophos Products**

1. Cloud Optix
2. Sophos Email
3. Sophos Mobile EAS Proxy

- **Sophos Protection Products**

Sophos is actively monitoring MTR customer accounts for post-exploit activity.

1. **Sophos Firewall**

   IPS signatures were published on December 11, 2021.

2. **Sophos Endpoint**

   IPS signatures were published on December 11, 2021.

3. **Sophos SG UTM**

   IPS signatures were published on December 11, 2021.

4. **Sophos XDR customers**

   Sophos XDR customers can use Sophos LiveQuery to. help identify vulnerable Log4j components in their environment.

5. **Sophos Recommendation**

   Sophos' recommendation is that if you have started patching, don't go back to the beginning again just yet. Finish patching your remaining systems with 2.16.0. This ensures a minimum version of at least 2.15.0 as quickly as possible to address the critical CVE-2021-44228 vulnerability. You can then go back and patch any 2.15.0 versions, so you have the same version everywhere.