Log4J Vulnerabilities - Microsoft Resolutions (Updated to 12 Dec 2021)

The information provided below is referred from https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and hunting-for-cve-2021-44228-log4j-2-exploitation/.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 12, 2021

- **Threat Level**

  High

- **Response to Log4j**

Microsoft's unified threat intelligence team, comprising the Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Threat Intelligence Team, RiskIQ, and the Microsoft Detection and Response Team (DART), among others, have been tracking threats taking advantage of CVE-2021-44228, remote code execution (RCE) vulnerability in Apache Log4j 2 referred to as "Log4Shell".

Microsoft has observed multiple threat actors leveraging the CVE-2021-44228 vulnerability in active attacks. Microsoft will continue to monitor threats taking advantage of this vulnerability and provide updates as they become available. To protect against these threats, they recommend that organizations follow the guidance detailed in succeeding sections.

- **Microsoft Security Solutions**

The following product help to against the log4j vulnerabilities.

1. **Microsoft 365 Defender**

   They have begun rolling out updates to the Threat and Vulnerability Management capabilities in Microsoft Defender for Endpoint to surface vulnerable Log4j library components

2. **Microsoft Defender Antivirus**

   Turn on cloud-delivered protection in Microsoft Defender Antivirus to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block the majority of new and unknown variants. Microsoft Defender Antivirus detects components and behaviors related to this threat as the following detection names

3. **Microsoft Defender for Endpoint**

   Users of Microsoft Defender for Endpoint can turn on the following attack surface reduction rule to block or audit some observed activity associated with this threat.

Block executable files from running unless they meet a prevalence, age, or trusted list criterion

4. **Microsoft Defender for Office 365**

   To add a layer of protection against exploits that may be delivered via email, Microsoft Defender for Office 365 flags suspicious emails (e.g., emails with the “jndi” string in email headers or the sender email address field), which are moved to the Junk folder.

5. **Microsoft Defender for Cloud**

   Microsoft Defender for Cloud’s threat detection capabilities have been expanded to surface ensure that exploitation of CVE-2021-44228 in several relevant security alerts.

6. **Microsoft Defender for IoT**

   Microsoft Defender for IoT has released a dedicated threat Intelligence update package for detecting Log4j 2 exploit

7. **Microsoft Sentinel**

   A new Microsoft Sentinel solution has been added to the Content Hub that provides a central place to install Sentinel specific content to monitor, detect, and investigate signals related to exploitation of the CVE-2021-44228 vulnerability.

8. **Azure Firewall Premium**

   Customers using Azure Firewall Premium have enhanced protection from the Log4j RCE CVE-2021-44228 vulnerability and exploit. Azure Firewall premium IDPS (Intrusion Detection and Prevention System) provides IDPS inspection for all east-west traffic and outbound traffic to internet. The vulnerability rulesets are continuously updated and include CVE-2021-44228 vulnerability for different scenarios including UDP, TCP, HTTP/S protocols

since December 10th, 2021.

9. **Azure Web Application Firewall (WAF)**

   Customers using WAF Managed Rules would have already received enhanced protection for the Log4j 2 vulnerability (CVE-2021-44228); no additional action is needed.

10. **Indicators of compromise(IOSc)**

    Microsoft Threat Intelligence Center (MSTIC) has provided a list of IOCs related to this attack and will update them with new indicators as they are discovered:
    https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/SampleData/Feeds/Log4j_IOC_List.csv