

Log4j vulnerability

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:35 AM PDT


Contents

- [Internal Reference](#)
- [RCA Template](#)

Internal Reference



<https://portal.microsofticm.com/imp/v3/incidents/details/277652055/home> 

RCA Template



Microsoft is aware of active exploitation of a critical Log4j Remote Code Execution vulnerability affecting various industry-wide Apache products. This vulnerability is in the open source Java component Log4J versions 2.0 through 2.14.1 (inclusive) and is documented in Apache [CVE-2021-44228](#) .

We are taking steps to keep customers safe and protected - including performing a cross-company assessment to identify and remediate any impacted Microsoft services. As of 13 December 2021, Microsoft is not aware of any impact to the security of our enterprise services and has not experienced any degradation in the reliability or availability of those services as a result of this vulnerability. However, we are still actively investigating utilization of Log4j in our services, and this determination may be subject to change at any given time based upon investigative findings. We will update this statement as the event warrants.

We are also **investigating for potential customer/partner impact. If we identify any customer/partner impact, we will notify the affected party.**

We recommend that customers review Apache [CVE-2021-44228](#)  and the Apache security advisory ([Apache Log4j Security Vulnerabilities](#) ) for details about the vulnerability and references to additional resources that can be used to remediate the issue in customer environments.

Guidance from Microsoft Please review the following guidance from Microsoft pertaining to this issue:


- **MSRC Blog:** [Microsoft's Response to CVE-2021-44228 Apache Log4j 2](#) 
- **Microsoft Security blog:** [Guidance for preventing detecting and hunting for CVE-2021-44228 log4j2 exploitation](#) 



Regarding Microsoft Defender:

- Microsoft Defender antivirus provides detections and protections for known malicious coin miner activity leveraging this exploit in build version **1.355.99.0** or higher. Customers utilizing automatic updates do not need to take additional action. Enterprise customers managing updates should select the new detection build or newer and deploy it across their environments.
- Microsoft Defender for Endpoint provides customers detection and alerts for possible Log4j exploitation. Alerts will be displayed as: "**Possible Log4j exploitation**".

- Turn on cloud-delivered protection and automatic sample submission on Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.

Regarding the Minecraft Java Edition:

- Minecraft customers who apply the fix are protected.
- Please see Minecraft Wiki for further details: Minecraft Wiki: [Java Edition 1.18.1 – Minecraft Wiki \(fandom.com\)](https://minecraft.fandom.com/wiki/Java_Edition_1.18.1) 

We encourage our customers to practice industry-standard best practices for security and data protection including embracing the **Zero Trust Security model** and adopting robust strategies to manage product security updates, endpoint security updates, and passwords. More information on **Zero Trust Security** is available at <https://aka.ms/zerotrust> . Additional information is available at <https://www.microsoft.com/en-us/security> .

How good have you found this content?



-