Template - Log4j vulnerability exploit aka Log4Shell IP IOC

Link to alert

**Description**

Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228.

**How to investigate**

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228'

**Classification**: Incident

User details

User:

Country or region:

Date:

Device:

IP address flagged by the query:

Location:

Application:

User agent:

Client App used:

**Remediation**

Block IP address (<https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Log4j_IOC_List.csv>)

User to release IP address from the device

Revoke session tokens to devices the user logged into

Reset password

Make sure the machine is completely updated and all your software has the latest patch.

Install and run Microsoft’s Malicious Software Removal Tool (see https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx).

Run Microsoft’s Autoruns utility and try to identify unknown applications that are configured to run at login (see https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx).

Run Process Explorer and try to identify unknown running processes (see <https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>).

Update all Log4j2 deployments to use **log4j-2.17.0** and apply the security updates for [CVE-2021-44228](https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2) and  [CVE-2021-45046](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046). Upgrade all products, applications and components that consume Log4j2. Apply all security updates for Log4J listed in this [advisory](https://logging.apache.org/log4j/2.x/security.html).