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: Apple

IP address flagged by the query:

Location:

Application:

User agent:

**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 mobile phone

Update OS of the mobile phone

Revoke session tokens to devices the user logged into

Reset password