Installing the Log4j Vulnerability Script in Barracuda RMM

https://campus.barracuda.com/doc/98217097/

This KB will help guide you through the process of installing the Log4j CVE-2021-44228 Vulnerability scanning script designed to enable partners to identify potential at-risk devices so that they may be patched and updated.

What is the Log4j CVE-2021-44228 Vulnerability and how are devices vulnerable? Log4j is an open-source library from Apache that is used the internet over in a myriad of software vendors. To better understand it, please see the following articles:

Apache   CNET   CNN   Microsoft

Installing the Log4j Vulnerability Script in Barracuda RMM

- Log into your **Barracuda RMM Service Center**
- Click on **Update Center**
- Select **Products**
- Then click on **Get More**
- In the **Search** Box type in Log4j and search
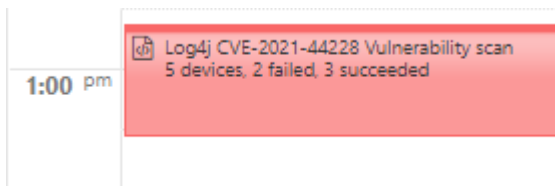- Select the Log4j CVE-2021-44228 Vulnerability scan script and **Install**

This will install the script into the automation library and will need to be run against devices. The Barracuda RMM Support team would like to caution, however, that you will want to run this script in batches of no more than 250 devices at a time . Please plan accordingly, as it running it broad-spectrum can cause automation issues.

Running the Log4j Vulnerability Script in Barracuda RMM scan

- Log into your **Barracuda RMM Service Center**
- Click on **Automation**
- Select **Calendar**
- Now select **Schedule**
- **Choose Item from Library** to execute
- Then search the name as **Log4j CVE-2021-44228 Vulnerability scan**
- **Add Devices** or Groups (limiting to 250 devices per automated task)
- **Schedule** a date and time for it to run

Understanding the results from the Log4j CVE-2021-44228 Vulnerability scan results

After the Log4j CVE-2021-44228 Vulnerability script has run, you will see the following information in your Automation Calendar:

Expanding the results will reveal which devices do not need any action (Succeeded) and those that will need to be looked at (Failed with Return Code 1):

From this list, select the Details to find out which program on the device is possibly at risk. Barracuda RMM Partners will want to work with their vendors in order to bring devices up to date and close the loop on this vulnerability. We encourage that this be done as soon as possible to minimize the impact overall. Logs are also hosted on each device under C:\ProgramData\BRMM_Log4JScan.txt to detail the scan results.

For More Information from BarracudaMSP about the Log4j CVE-2021-44228 Vulnerability, please read our latest post here: https://www.barracuda.com/company/legal/trust-center
 and http://download.mw-rmm.barracudamsp.com/PDF/12.5.0/RN_RMM_Log4j_vulnerability_script_EN.

[pdf](#)

Figures

1. pasted image 0.png
2. pasted image 0 (1).png