NATILIK

London | New York | Sydney

VQ COMMUNICATIONS

VQ Communications Impact Statement and Mitigation Steps

On December 13, 2021, we issued a security advisory regarding a critical severity CVE that impacted an Apache library (Log4j 2) and anything which used this. This includes Elasticsearch (ES). Elasticsearch is a component within VQ Conference Manager.

We got to work in-house testing to better understand the issue, its implications and the impact it has on VQCM VMs. One of the conclusions from this analysis and testing was that it would be non-trivial for the CVE to be successfully exploited because of VQCM's logging architecture. Especially for an external facing attacker.

Whilst this gives a degree of assurance, we strongly recommend customers apply a mitigation script we have created. The script follows mitigation advice from Elasticsearch. Details of how to get the script and how to run it can be found below.

In addition, Elasticsearch will be producing a new version of Elasticsearch (7.16.1) which removes the affected module. VQCM 3.9 is due mid-January and will contain Elasticsearch 7.16.1.

The guidance is:

- Download and apply the mitigation script as soon as possible.
- Plan on upgrading to VQCM 3.9 in January (due 1/17/2022)
- Minimize public internet exposure wherever possible. If you do need to expose a public service, ensure only HTTPS ports are open and use a reverse proxy or equivalent.

Instructions for downloading and installing the mitigation script

Please note this script **will bring the system down**, so it is recommended to be run out of working hours.

- Navigate to the https://www.vqcomms.com/resources/ page, log in and download the "log4j2-cve.zip" file from the "CVE-2021-44228 Mitigation Script" category.
- Enable SSH from the CM-Admin page (port 1234) under the "Start / Manage / SSH Access" section, and create an SSH user if you don't already have one (Note: SSH is enabled if the button shows "Disable SSH access").
- Using WinSCP or SCP, copy the "log4j2-cve.zip" file on the VQCM Virtual Machine (VM), under the home directory of your SSH user.
- Open an SSH session using Putty (or similar tool) with the VQCM VM, authenticating with the same SSH user.
- Run the following commands:
- unzip log4j2-cve.zip
- chmod +x log4j2-cve.sh
- sudo ./log4j2-cve.sh

9A Devonshire Square, London EC2M 4YN

T +44 203 597 8000 | E hello@natilik.com

natilik.com

Natilik Limited
Registered in England & Wales Number: 595 4905 | VAT 894 3202 16

- This command will ask you for your password to escalate privileges, this is the same password as the SSH user you are logged in as.
- The tool will run for a moment (10-15 mins, could be more depending on how much data your system has). If it runs successfully to the end, it will output **"SUCCESS the mitigation has been applied":**

PLAY RECAP
****
****
****

localhost : ok=13 changed=7 unreachable=0 failed=0 skipped=8 rescued=0 ignored=0

All pods are running, exiting

usename

---

postgres

(1 row)

ALTER ROLE

~~~

SUCCESS the migitation has been applied

~~~

If you see the **SUCCESS** message, the mitigation has been applied successfully. If you see the **"ERROR the mitigation was NOT applied"**, please contact VQ support at support@vqcomms.com, with as much information as possible.

Which versions of VQ can I use the mitigation script with?

- Versions 3.6, 3.7 and 3.8; please run the mitigation script.
- For 3.x versions 3.5 and below, please contact support@vqcomms.com.