

# 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/DetailView.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 -> Mobile
- 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<sql>>
- For example, to change the admin password to \$attacker\$, type:  
[https://<AppMgrHost>:8443/showresource.do?method=showResourceForResourceID&resourceid=99999%3bUPDATE%20AM\\_UserPasswordTable%20SET%20password%20=%20\\$attacker%241de45bdd8d5df3028bbcc4e1](https://<AppMgrHost>:8443/showresource.do?method=showResourceForResourceID&resourceid=99999%3bUPDATE%20AM_UserPasswordTable%20SET%20password%20=%20$attacker%241de45bdd8d5df3028bbcc4e1)

## 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](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 ZOH0 bugbounty webform  
12/18/2020 - Tenable resubmitted report via web form  
12/21/2020 - ZOH0 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

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](mailto:advisories@tenable.com)

## 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.



## 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



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

© 2022 Tenable®, Inc. All Rights Reserved



