



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



SEC Consult SA-20200122-0 :: Reflected XSS in ZOHO ManageEngine ServiceDeskPlus

From: SEC Consult Vulnerability Lab <research () sec-consult.com>

Date: Wed, 22 Jan 2020 12:10:06 +0100

SEC Consult Vulnerability Lab Security Advisory < 20200122-0 >

```
=====
title: Reflected XSS
product: ZOHO ManageEngine ServiceDeskPlus
vulnerable version: <= 11.0 Build 11007
fixed version: 11.0 Build 11010
CVE number: CVE-2020-6843
impact: medium
homepage: https://www.manageengine.com/products/service-desk/
found: 2019-12-01
by: Johannes Kruchem (Office Vienna)
SEC Consult Vulnerability Lab

An integrated part of SEC Consult
Europe | Asia | North America

https://www.sec-consult.com
=====
```

Vendor description:

"ServiceDesk Plus is a game changer in turning IT teams from daily fire-fighting to delivering awesome customer service. It provides great visibility and central control in dealing with IT issues to ensure that businesses suffer no downtime. For 10 years and running, it has been delivering smiles to millions of IT folks, end users, and stakeholders alike."

Source: <https://www.manageengine.com/products/service-desk/>

Business recommendation:

The vendor published a patch for ServiceDesk Plus with service pack 11010.

It is recommended to install the patch with the included patcher. An in-depth security analysis performed by security professionals is highly advised, as the software may be affected from further security issues.

Vulnerability overview/description:

1) Reflected Cross-Site Scripting (CVE-2020-6843)
A parameter of the module called "geti18nkey" reflects unfiltered user input if it is changed. The corresponding request is frequently sent in the background if a pre-configured network scan was started.

Proof of concept:

1) Reflected Cross-Site Scripting (CVE-2020-6843)
To reproduce the issue visit this URL authenticated as administrator:
[http://\\$IP:8080/CustomReportHandler.do?module=geti18nkey&key=<img%20src%20onerror%3dalert\(1\)>](http://$IP:8080/CustomReportHandler.do?module=geti18nkey&key=<img%20src%20onerror%3dalert(1)>)

How the parameter was found:

1) Authenticate as administrator and add an IP range in Admin -> Networkscan.
2) Click the "play" button next to the created IP range to start the scan.
3) To check the status of a started network scan frequent requests like

"[http://\\$IP:8080/CustomReportHandler.do?module=geti18nkey&key=sdp.admin.network.listview.discoverystatus.scanned&sdpcsrparam=<%someUUID%>](http://$IP:8080/CustomReportHandler.do?module=geti18nkey&key=sdp.admin.network.listview.discoverystatus.scanned&sdpcsrparam=<%someUUID%>)" are sent to the server.
4) The value of the "key" parameter will be reflected if you change a single character. The "sdpcsrparam" isn't needed in order to trigger the XSS.
5) XSS can thus be exploited by calling
"[http://\\$IP:8080/CustomReportHandler.do?module=geti18nkey&key=<img%20src%20onerror%3dalert\(1\)>](http://$IP:8080/CustomReportHandler.do?module=geti18nkey&key=<img%20src%20onerror%3dalert(1)>)"

Vulnerable / tested versions:

The following versions have been tested which were the latest versions available at the time of the test:

- 10.5
- 11.0 Build 11007

Vendor contact timeline:

2019-12-05: Contacting vendor through ManageEngine Security Response Center (MESRC)
Uploaded security advisory to bugbounty.zoho.com
2019-12-09: Vendor promised to fix the vulnerability.
2020-01-08: Reported issue has been fixed in service pack 11010.
2020-01-22: Public release of security advisory.

Solution:

The vendor provides an updated version which should be installed immediately.
<https://www.manageengine.com/products/service-desk/download.html>

The vendor also provided a link to their readme about the new release:
<https://www.manageengine.com/products/service-desk/readme.html#11010>

Workaround:

None

Advisory URL:

<https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html>

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab

The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. It ensures the continued knowledge gain of SEC Consult in the field of network and application security to stay ahead of the attacker. The SEC Consult Vulnerability Lab supports high-quality penetration testing and the evaluation of new offensive and defensive technologies for our customers. Hence our customers obtain the most current information about vulnerabilities and valid recommendation about the risk profile of new technologies.

Interested to work with the experts of SEC Consult?
Send us your application <https://www.sec-consult.com/en/career/index.html>

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices <https://www.sec-consult.com/en/contact/index.html>

Mail: [research at sec-consult dot com](mailto:research@sec-consult.com)
Web: <https://www.sec-consult.com>
Blog: <http://blog.sec-consult.com>
Twitter: https://twitter.com/sec_consult

EOF Johannes Kruchem / @2020

Attachment: [gmime.p7s](#)

Description: S/MIME Cryptographic Signature





Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

Current thread:

SEC Consult SA-20200122-0 :: Reflected XSS in ZOHO ManageEngine ServiceDeskPlus SEC Consult Vulnerability Lab (Jan 22)

Site Search

Nmap Security Scanner	Npcap packet capture	Security Lists	Security Tools	About		
Ref Guide	User's Guide	Nmap Announce	Vuln scanners	About/Contact		
Install Guide	API docs	Nmap Dev	Password audit	Privacy		
Docs	Download	Full Disclosure	Web scanners	Advertising		
Download	Npcap OEM	Open Source Security	Wireless	Nmap Public Source License		
Nmap OEM		BreachExchange	Exploitation			