ZOHO ManageEngine ServiceDeskPlus 11.0 Build 11007 Cross Site Scripting

Authored by Johannes Kruchem | Site sec-consult.com

Posted Jan 22, 2020

ZOHO ManageEngine ServiceDeskPlus versions 11.0 Build 11007 and below suffer from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2020-6843
SHA-256 | f632ef85f28ad70bb9342601a5f35a98d661dd706019e37f2cc899fa7c91121f Download | Favorite | View

Related Files

Change Mirror Download

```
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 "getil8nkey" 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=getil8nkey&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://$IP:8080/CustomReportHandler.do?
module=getil8nkey&key=sdp.admin.network.listview.discoverystatus.scanned&sdpcsrfparam=<%someUUID%>"
   are sent to the server.
4) The value of the "key" parameter will be reflected if you change a single character.
   The "sdpcsrfparam" isn't needed in order to trigger the XSS.
5) XSS can thus be exploited by calling
   "http://$IP:8080/CustomReportHandler.do?module=getil8nkey&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.
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- Older

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
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
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF Johannes Kruchem / @2020
```


Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed