Emerson Smart Wireless Gateway 1420 4.6.59 Privilege Escalation

Authored by Harsha Bhat, Unmesh Guragol, Anish Mitra

Posted Mar 9, 2021

Emerson Smart Wireless Gateway version 1420 4.6.59 suffers from a privilege escalation vulnerability.

tags | exploit
advisories | CVE-2020-19417
SHA-256 | dc63f3b266b6fd679d8ed4e34ead07abc06aad6afdaa65e428b296c34a9cecd8

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Title: Privilege Escalation
Product: Emerson Smart Wireless Gateway
Vendor Homepage: http://emerson.com
Vulnerable Version: 1420 4.6.59
CVE Number: CVE-2020-19417
Authors: Harsha Bhat Anish Mitra and Unmesh Guragol
Timeline:
2019-08-02 Disclosed to the vendor
2019-08-22 Vendor confirmed that the vulnerability was identified
internally and a fix was released in the latest version of firmware

1. Vulnerability Description

Emerson Smart Wireless Gateway 1420 4.6.59 allows non-privileged users
(such as the default account 'maint') to perform administrative tasks by
sending specially crafted HTTP requests to the application.

2. PoC

The PoC explained below is to perform an action accessible ideally only to
an 'administrator' account
Step 1: Using a proxy tool such as Burp Suite, capture an original request
that sets the login banner on the device from a legitimate 'administrator'
account.
Step 2: Logout from the application and login with a low privilege user
account such as 'maint'. This account does not have privileges to set the
login banner.
Step 3: Replay the original request from 'Step 1' after replacing session
ID of 'administrator' account to that of 'maint' account.

Observe that the application, without validating the permissions set for
'maint' account sets the login banner via the low-privilege account.


3. Solution

The vendor provides an updated version of firmware which should be
installed immediately.

CAUTION - This message may contain privileged and confidential information
intended only for the use of the addressee
named above. If you are not the intended recipient of this message you are
hereby notified that any use, dissemination,
distribution or reproduction of this message is prohibited. If you have
received this message in error please notify
The Missing Link immediately. Any views expressed in this message are those
of the individual sender and may not
necessarily reflect the views of The Missing Link.
```

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