packet storm
what you don't know can hurt you

Search ...

Emerson Smart Wireless Gateway 1420 4.6.59 Missing Authentication

Authored by Harsha Bhat, Unmesh Guragol, Anish Mitra   Posted Mar 9, 2021

Emerson Smart Wireless Gateway version 1420 4.6.59 suffers from a missing authentication vulnerability.

tags | exploit
advisories | CVE-2020-19419
SHA-256 | 06aa33191140047b5e8717710ba3b1dbdfe6c9620cc5e0b31b03529c81139fc0   **Download** | **Favorite** | **View**

Related Files

Share This

Like   Twee   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
Title: Missing access controls
Product: Emerson Smart Wireless Gateway
Vendor Homepage: http://emerson.com
Vulnerable Version: 1420 4.6.59
CVE Number: CVE-2020-19419
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

Incorrect Access Control in Emerson Smart Wireless Gateway 1420 4.6.59
allows remote attackers to obtain sensitive information (device log files)
on the administration console.

2. PoC

The PoC explained below is to obtain device logs without authentication.
The following requests will retrieve device log files stored on the device.

Access the following URL without authenticating into the administrator
console:
https://192.168.0.1/servlet/hartserver.txt

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

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

packet storm

© 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