Sagemcom F@ST 5280 Privilege Escalation

Authored by Ryan Delaney | Posted Sep 1, 2020

Sagemcom F@ST 5280 routers using firmware version 1.150.61, and possibly others, have an insecure deserialization vulnerability that allows any authenticated user to perform a privilege escalation to any other user. By making a request with valid sess_id, nonce, and ha1 values inside of the serialized session cookie, an attacker may alter the user value inside of this cookie, and assume the role and permissions of the user specified. By assuming the role of the user internal, which is inaccessible to end users by default, the attacker gains the permissions of the internal account, which includes the ability to flash custom firmware to the router, allowing the attacker to achieve a complete compromise.

tags | exploit
advisories | CVE-2020-24034
SHA-256 | b749b45a358358330f8fd5f3cec1a2eb0a30872b9d8f5cd95aaf47010c1890ef | Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror | Download

```
<!--
# Exploit Title: Sagemcom router insecure deserialization > privilege
escalation
# Date: 08-31-2020
# Exploit Author: Ryan Delaney
# Author Contact: ryan.delaney () owasp org
# Author LinkedIn: https://www.linkedin.com/in/infosecrd/
# Vendor Homepage: https://sagemcom.com/en
# Software Link: N/A (F@ST 5280 firmware not published)
# Version: F@ST 5280 router, F/W 1.150.61, possibly others
# Tested on: F@ST 5280 router, F/W 1.150.61
# CVE: CVE-2020-24034

1. Description

Sagemcom F@ST 5280 routers using firmware version 1.150.61,
and possibly others, have an insecure deserialization vulnerability
that allows any authenticated user to perform a privilege escalation
to any other user. By making a request with valid sess_id, nonce,
and ha1 values inside of the serialized session cookie, an attacker may
alter the user value inside of this cookie, and assume the role and
permissions of the user specified. By assuming the role of the user
'internal', which is inaccessible to end users by default, the attacker
gains the permissions of the 'internal' account, which includes the
ability to flash custom firmware to the router, allowing the attacker
to achieve a complete compromise.

Note that the 'internal' account is disabled and hidden by default, and the
primary administrative account ('admin'), lacks the permission to
flash custom firmware to the device, meaning that an attacker
exploiting this vulnerability obtains access exceeding that of
the legitimate, authorized system administrator.

2. Proof of Concept

Log in as a valid user (default is admin:admin). Retrieve the 'session'
cookie. Simply change the only occurrence of the string "admin" within
the cookie to "internal", and make a new request with this modified cookie.
If you decode the cookie, you will note this is the 4th key value pair
inside of the cookie, where the key is "user", and the value is "admin".

3. Solution

This vulnerability is only exploitable with a valid existing session.
Changing the administrative password to a strong, non-default value,
and ensuring that TLS certificate has the correct fingerprint will
help prevent attackers from obtaining a valid existing session.

-->
```


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

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