tenable

Grandstream UCM62xx Multiple SQL Injections

Medium

← View More Research Advisories

Synopsis

While investigating the Grandstream UCM6202 IP PBX, Tenable discovered a few SQL injections that an unauthenticated remote attacker could use to obtain user passwords.

CVE-2020-5723: Cleartext Storage of Sensitive Information (CWE-312)

The UCM6200 series stores unencrypted user passwords in an SQLite database. This could allow an attacker to retrieve all passwords and possibly gain elevated privileges.

```
/ # /app/asterisk/bin/sqlite3 ./cfg/etc/ucm_config.db
SQLite version 3.26.0 2018-12-01 12:34:55
Enter ".help" for usage hints.
sqlite> SELECT user_password FROM users;
LabPass1%
xN8r2jE8V8NmR
zY5SLrb8!bj9
pC68lLzT%24d
rU8Fwb70X128
k@4Q2x%23!H77j
w!6qk6~fkXktk
g*3058991%7LuC!a
lX0CA#br2h9
sqlite>
```

CVE-2020-5724: Unauthenticated Remote Blind SQL Injection

The webserver's websockify endpoint is vulnerable to SQL injection when the *challenge* action is invoked. The username provided by the unauthenticated remote attacker is used to build an SQL query into the users table. Furthermore, successful queries and unsuccessful queries generate different responses from the server. As such, an unauthenticated remote attacker can recover user passwords.

A proof of concept can be found in our GitHub repository.

CVE-2020-5725: Unauthenticated Remote Blind SQL Injection

The webserver's websockify endpoint is vulnerable to SQL injection when the *login* action is invoked. The username provided by the unauthenticated remote attacker is used to build an SQL query into the users table. As such, by using time based attacks, an unauthenticated remote attacker can recover user passwords.

A proof of concept can be found in our GitHub repository.

CVE-2020-5726: Unauthenticated Remote SQL Injection via CTI

The CTI server on port 8888 is vulnerable to SQL injection when the *challenge* action is invoked. The username provided by the unauthenticated remote attacker is used to build an SQL query into the users table. Furthermore, successful queries and unsuccessful queries generate different responses from the server. As such, an unauthenticated remote attacker can recover user passwords

A proof of concept can be found in our GitHub repository.

Solution

Upgrade to 1.0.20.22 or newer.

Additional References

http://firmware.grandstream.com/Release_Note_UCM6xxx_1.0.20.22.pdf
https://github.com/tenable/poc/blob/master/grandstream/ucm62xx/websockify_challenge_injection.py
https://github.com/tenable/poc/blob/master/grandstream/ucm62xx/websockify_login_injection.py
https://github.com/tenable/poc/blob/master/grandstream/ucm62xx/cti_injection.py

Disclosure Timeline

March 23, 2020 - Tenable reports unauth password disclosure websockify SQL injection.
March 24, 2020 - Grandstream acknowledges Tenable and escalates the report.
March 25, 2020 - Grandstream asks Tenable to test against 1.0.20.20.
March 25, 2020 - Tenable replies 1.0.20.20 is vulnerable.
March 27, 2020 - Tenable reports two additional SQL injections.
March 27, 2020 - Grandstream acknowledges and asks which version Tenable tested against.
March 27, 2020 - Tenable replies 1.0.20.20
March 30, 2020 - Grandstream informs Tenable that they've patched the issues in 1.0.20.22.

CVE-2020-5726
Tenable Advisory ID: TRA-2020-17
Credit: Jacob Baines

CVSSv2 Base / Temporal Score: 5.0 / 4.1
CVSSv2 Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Affected Products: Grandstream UCM62xx 1.0.20.20 and below
Risk Factor: Medium

Advisory Timeline

March 30, 2020 - Initial Release