SA-2023-01

Notification Date: October 18, 2023

SECURITY ADVISORY

v2 Products May Generate Insufficiently Random Keys

Summary

Unlike other ICR products, the v2 products don't have a hardware random number generator (RNG) and rely on pseudorandom generators. This approach may in rare situations lead to insufficiently random keys, which are not secure and allow an attacker to determine the private key from a device's certificate.

Issue Description

Linux devices have an unlimited source of random numbers (`/dev/urandom`) that uses a pseudorandom generator seeded from an entropy pool. During the first system start the `/dev/urandom` is used to generate the SSH and HTTPS keys and certificates.

Once properly initialized, the `/dev/urandom` on all platforms provide sufficiently random numbers that pass the FIPS 140-2 tests of the rngtest tool with an 1‰ error.

```
# rngtest -c 5000 < /dev/urandom
rngtest 6.16
Copyright (c) 2004 by Henrique de Moraes Holschuh
This is free software; see the source for copying conditions.  There is NO warranty;
                   not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

rngtest: starting FIPS tests...
rngtest: bits received from input: 100000032
rngtest: FIPS 140-2 successes: 4996
rngtest: FIPS 140-2 failures: 4
rngtest: input channel speed: (min=3.828; avg=63.787; max=66.227)Mibits/s
rngtest: FIPS tests speed: (min=2.845; avg=10.420; max=10.740)Mibits/s
rngtest: Program run time: 10735744 microseconds
```

When the system starts the entropy may be in an unpredictable state and devices without a hardware random generator may generate insufficiently random numbers and thus weak private keys. When two private RSA keys are insufficiently random, an attacker can easily determine the private from a device's certificate, as described in [1] and [2].

Advantech Czech s.r.o.
Sokolská 71, Kerhartice
562 04 Ústí nad Orlicí
Czech Republic

Tel: +420 465 524 421
E-mail: cellular.info@advantech.cz
Web: www.advantech.cz

IČO: 24148661
DIČ: CZ24148661

[1] Heninger, Durumeric, Wustrow, Halderman: Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices, 21st USENIX Security Symposium (USENIX Security 12), 2012.

[2] Nadia Heninger: Random number generation done wrong, Wr0ng Workshop, Paris, May 2017.

The risk of generating weak keys is higher on firmware prior 6.2.0, because the `/dev/urandom` used since then will wait until at least 128 bits of entropy has been accumulated in the entropy pool.

Affected Products

All v2 devices lacking a hardware random number generator are impacted: Bivias v2 HC, Bivias v2 HH, Bivias v2 LC, Bivias v2 LH, Bivias v2 LL, CR10 v2, ER75i v2, LR77 v2, LR77 v2 Libratum, RR75i v2, Spectre LTE, Spectre RT, UCR11 v2, UR5i v2, UR5i v2 Libratum, XR5i v2, XR5i v2E, ICR-2100, and ICR-2300. **All of these products have reached their End of Life status and are no longer being manufactured.**

The risk of insufficiently random keys is higher for firmware prior 6.2.0, released in 2019.

Solution

- Improved `/dev/urandom` is included since the firmware 6.2.0. Users of all products are strongly recommended to always use the latest firmware.
- Firmware upgrade preserves the existing keys. If you are still using the default keys generated back in 2019 or earlier, change (rotate) your keys:
  - For the HTTP Service select *Generate a new certificate*;
  - for the SSH Service select *Generate a new SSH key* and use a key length of at least 2048.
- In any case change (rotate) the HTTPS and SSH keys regularly. It reduces the risks of key theft and prevents long-term key-based attacks.
- Also, the device admin interfaces (HTTP, SSH), including the HTTPS interface with default self-signed certificates should not be open to the public internet. Make sure the admin interfaces are accessible from the trusted LAN only.

Acknowledgement

The vulnerable devices have been discovered by Andrew Chi, David McGrew and Brandon Enright form Cisco Systems.

Revision History

2023-10-18 Advisory published