Verizon 4G LTE Network Extender Weak Credentials Algorithm

Title: Verizon 4G LTE Network Extender Weak Credentials Algorithm
Advisory ID: ZSL-2022-5701
Type: Local/Remote
Impact: Security Bypass
Risk: (3/5)
Release Date: 13.04.2022

Summary

An LTE Network Extender enhances your indoor and 4G LTE data and voice coverage to provide better service for your 4G LTE mobile devices. It's an extension of our 4G LTE network that's placed directly in your home or office. The LTE Network Extender works with all Verizon-sold 4G LTE mobile devices for 4G LTE data service and HD Voice-capable 4G LTE devices for voice service. This easy-to-install device operates like a miniature cell tower that plugs into your existing high-speed broadband connection to communicate with the Verizon wireless network.

Description

Verizon's 4G LTE Network Extender is utilising a weak default admin password generation algorithm. The password is generated using the last 4 values from device's MAC address which is disclosed on the main webUI login page to an unauthenticated attacker. The values are then concatenated with the string 'LTEFemto' resulting in something like 'LTEFemtoD080' as the default Admin password.

Vendor

Verizon Communications Inc. - https://www.verizon.com

Affected Version

GA4.38 - V0.4.038.2131

Tested On

lighttpd-web

Vendor Status

[17.02.2022] Vulnerability discovered.
[23.02.2022] Vendor contacted.
[24.02.2022] Vendor responds asking more details.
[24.02.2022] Sent details to the vendor.
[06.03.2022] Asked vendor for status update.
[07.03.2022] Vendor has sent the report over to product security team. As soon as they have time to assess, vendor will give us an update.
[12.04.2022] No response from the vendor.
[13.04.2022] Public security advisory released.

PoC

Exploit.js

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://packetstormsecurity.com/files/166712/
[2] https://cxsecurity.com/issue/WLB-2022040047
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/224210
[4] https://www.exploit-db.com/exploits/50875
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29729
[6] https://nvd.nist.gov/vuln/detail/CVE-2022-29729

Changelog

[13.04.2022] - Initial release
[14.04.2022] - Added reference [3]
[20.04.2022] - Added reference [4]
[29.05.2022] - Added reference [5] and [6]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Rete mirabilia**
- **We Suggest**
- **Profiles**

- Site Meter