ZYXEL

www.Zyxel.com

Zyxel security advisory for the kr00k vulnerability

CVE: CVE-2019-15126

Summary

A vulnerability, dubbed as kr00k, was identified in Broadcom and Cypress WiFi chips that could allow specifically timed and handcrafted traffic to cause internal errors (related to state transitions) in a wireless LAN device, which could lead to unauthorized decryption of some WPA2-encrypted traffic.

What is the vulnerability?

Based on the preliminary analysis from Broadcom, the vulnerability is a possible transmission of a few frames without proper MAC level encryption, and currently there is no known way to exploit this particular vulnerability to

- discover the original security key,
- inject data frames,
- cause buffer overflows, corrupt memory or,
- execute arbitrary code on the affected device.

Given these factors, the risk is limited to information exposure in the few data frames that can be decrypted by a hacker. Additionally, this attack does not compromise the integrity of end-to-end (SSL) encryption that is common for sensitive exchanges.

In conclusion, though the vulnerability may be easy to exploit, it is not expected to result in significant security lapses. The National Vulnerability Database of National Institute of Standards and Technology (NIST NVD) of the United States has rated the severity level of this vulnerability at "**3.1 Low**" on a scale of 10.

What products are vulnerable—and what should you do?

After a thorough investigation, we've identified the vulnerable products that are within their warranty and support period, as shown in the table below. For optimal protection, we urge users to install the firmware patches as soon as they become available.

Affected model	Standard firmware availability
EMG6726	V513ABNP5C0 in Aug
VMG4927/VMG3927	V513ABLY5C0 in Aug
EX5510-B0	V515ABQX1C0 in April
VMG4825/VMG9823/VMG3925	TBD
P-660HN-51	TBD
VSG1432/VSG1435	EOL/ End of software support
VMG4325/VMG4380/ VMG4381	EOL/ End of software support
P-873HNU-51B	EOL/ End of software support

Got a question or a tipoff?

Please contact your local service rep for further information or assistance. If you've found a vulnerability, we want to work with you to fix it—contact security@zyxel.com.tw and we'll get right back to you.

Source

https://www.eset.com/int/kr00k/