eMazzanti technologies®
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

eMazzanti Technologies Urges Customers to download KRACK Wi-Fi Vulnerability Patch

NYC area IT security consultant also warns the public to take extra precautions to avoid data loss from new KRACK Wi-Fi data security threat

Hoboken, New Jersey -- (Cision) November 2, 2016 — eMazzanti Technologies, a NYC area IT consultant and MSP, issued a warning today regarding several recently revealed WPA/WPA2 encryption protocol vulnerabilities that affect countless Wi-Fi enabled devices worldwide.

The company urges customers with WatchGuard network security hardware and others to download patches to fix the vulnerabilities in their equipment. They also urge all business and home computer users to take extra precautions to avoid being victimized by the KRACK Wi-Fi encryption vulnerability. The recently discovered vulnerability allows hackers to steal user IDs and passwords.

“KRACK is potentially devastating to Wi-Fi users,” stated Almi Dumi, Project Lead, eMazzanti Technologies. “We strongly advise WatchGuard users to download the latest security patches for their Wi-Fi routers and access points. We also urge our customers and others to take additional steps to avoid losing data.”

Here is the text of the warning:

KRACK Wi-Fi Vulnerability Warning

“eMazzanti Technologies wants to bring to your attention a very serious threat that is affecting Wi-Fi networks worldwide.

KRACK, the newest Wi-Fi threat, stands for Key Reinstallation AttACK. It takes advantage of a router encryption flaw to force one-time log-ins to be re-used. This gives hackers an opportunity to decode and steal personal information like credit card and banking information, passwords and photos.

Since personal data can be sold, hackers will be exploiting this vulnerability wherever possible. Public places offer more targets, but an attack can succeed on any unpatched wireless network secured by WPA encryption.”

Steps for eMazzanti customers with WatchGuard Equipment

Many of eMazzanti’s customers employ WatchGuard Wi-Fi equipment in their networks. WatchGuard has published the information below about how to protect your network from KRACK vulnerabilities. In general, the recommended patches protect Wi-Fi users in various scenarios, including from unpatched client devices.

1. Update to the latest (10/30/17) access point (AP) firmware - WatchGuard will provide patches for all supported APs and tabletop appliances with embedded wireless APs.

2. Enable “Mitigate WPA/WPA2 key reinstallation vulnerability in clients” feature. The AP can compensate for the unpatched clients with this setting enabled. Mitigation is recommended only until all clients are patched.

   In a small percentage of cases, mitigation may exacerbate client connectivity issues in environments already suffering from weak signal coverage or high interference.

3. Alternatively, enable “AP MAC Spoofing Prevention” setting in Wi-Fi Cloud WIPS policy.

See WatchGuard Product and Support News for additional details.

Additional Precautions

With KRACK, the hacker must be within the transmission range of your Wi-Fi router or access point. That makes public Wi-Fi more prone to attack than home networks.

- Take precautions away from the office or home and avoid connecting to public Wi-Fi.

- As an alternative to public Wi-Fi, use your work or personal phone as a hot spot. If it is encrypted and patched, no one can gain access to your information.

- Download the latest updates sent by your equipment vendor or device manufacturer. Even though they come out after a threat is reported, install them ASAP! If not patched, these vulnerabilities will remain and your chances of suffering data loss increases.

Keeping up with threats to sensitive data requires that individuals and organizations stay vigilant. Accordingly, anyone charged with data security who is unsure about what to do may call the IT security professionals at eMazzanti Technologies

Related resource information:

Employee Devices Bring Added Security Concerns

The best way to prepare for disasters and security breaches

About eMazzanti Technologies

eMazzanti’s team of trained, certified IT experts rapidly deliver cloud and mobile solutions, multi-site implementations, 24×7 outsourced network management, remote monitoring and support to increase productivity, data security and revenue growth for clients ranging from professional services firms to high-end global retailers.

eMazzanti has made the Inc. 5000 list six years running, is a 2015, 2013 and 2012 Microsoft Partner of the Year, and a 5X WatchGuard Partner of the Year. Contact: 1-866-362-9926, info@emazzanti.net or emazzanti.net Twitter: @emazzanti   Facebook: Facebook.com/emazzantitechnologies.

2015 I 2013 I 2012 Microsoft
Partner of the Year

WatchGuard
5x WatchGuard
Partner of the Year

Inc.500 ||| 5000
2016 I 2015 I 2014 I 2013 I 2012 I 2011 I 2010

hp Partner of the Year

ShoreTel Sky
Partner of the Year