eMazzanti Technologies Issues DROWN Attack Warning

NYC area IT security consultant urges organizations to check and update servers to avoid data loss in light of security threat affecting up to 33% of HTTPS servers

Hoboken, New Jersey -- (Cision) March 11, 2016 — eMazzanti Technologies, a NYC area IT consultant and MSP, issued a security warning today regarding a threat to encrypted server traffic which is usually considered to be secure. Any data exchanged with vulnerable servers is at risk.

The vulnerability, called DROWN, was discovered by an international team of researchers and made public by the Department of Homeland Security, US-CERT or United States Computer Emergency Readiness Team on March 1, 2016. According to the US-Cert notice, DROWN is a potential threat in up to 33% of all HTTPS servers.

eMazzanti is urging organizations to check their servers for the vulnerability to prevent hackers from stealing sensitive data. Any data transmitted to or from a vulnerable server can be compromised, including passwords, credit card data, and other sensitive information.

"With DROWN out in the open, hackers are sure to exploit it," stated Almi Dumi, Project Lead, eMazzanti Technologies. "We urge our customers and others to take the necessary steps to prevent hackers from stealing their sensitive data. Every HTTPS server should be checked."

Here is the full text of the warning:

DROWN Attack Warning

"eMazzanti Technologies wants to bring to your attention a very serious threat, a server vulnerability called DROWN, that puts up to one third of all HTTPS servers at risk. DROWN stands for Decrypting RSA with Obsolete and Weakened eNcryption.

DROWN affects HTTPS and other services that rely on SSL and TLS cryptographic protocols for Internet security. These protocols prevent third parties from reading Internet communications used by everyone to browse websites, shop online and send email and instant messages.

Attackers use DROWN to break the encryption and steal sensitive information, including passwords, credit card numbers, critical business data or financial information. Many popular websites, even small business websites, as well as mail servers, and other TLS-dependent services are at risk.

eMazzanti urges businesses and organizations to have their servers checked by professionals for the vulnerability and updated to avoid being victimized by hackers who have the ability to exploit the vulnerability to decipher data. Any data exchanged with a vulnerable server is at risk.

There are no practical measures or software that users can employ at the browser level to prevent a DROWN attack. Only server operators and IT security professionals can take the necessary action to prevent an attack."

Additional Information about Drown

Modern servers and clients use the TLS encryption protocol. However, due to misconfigurations, many servers also still support SSLv2, a 1990s-era predecessor to TLS, making them vulnerable to DROWN. Even servers that don't support SSLv2 may be at risk if they use the same private keys as other vulnerable servers in the organization.

Researchers have been able to execute the attack against some flawed OpenSSL encryption software in less than a minute using a single PC. Even for servers that don't have those flaws, a successful attack against any SSLv2 server can be conducted in under eight hours with less than $500 of computing resources.

The Word is Out, Take Action Now

Security researchers have stated that they have no evidence that DROWN has been exploited by hackers prior to the US-CERT alert. However, since the details of the vulnerability have been made public, cyber criminals may strike at any time. Experts recommend taking preventative action as soon as possible.

A server does not need to be actively using SSLv2 to be vulnerable. Simply allowing SSLv2 permits an attacker to decrypt up-to-date TLS connections between clients and servers by probing any server that supports SSLv2 using the same private key.

PCI Compliant Servers also at Risk

Even certified PCI compliant HTTPS servers may be at risk if a private key is reused on another server (such as an email server) that supports SSLv2. DROWN allows the PCI compliant server to be attacked even though SSL has been disabled on that server. Experts recommend manually inspecting all servers that use the same private key.

The DROWN vulnerability is another negative consequence of the way cryptography was weakened by 1990s U.S. government policies that restricted exporting strong cryptography. Although these restrictions were relaxed nearly 20 years ago, the weakened cryptography remains and continues to be supported by many servers.

Professional Help Available

eMazzanti's trained IT security experts stand ready to assist organizations as they deal with the DROWN vulnerability and other security issues. New Internet threats appear daily. A security-first

mindset and proactive approach is necessary to keep networks and assets safe in today's evolving threat landscape.

Related resource information:

Fixing the HTTPS Security Blind Spot

eMazzanti Technologies Issues Locky Ransomware Warning

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.