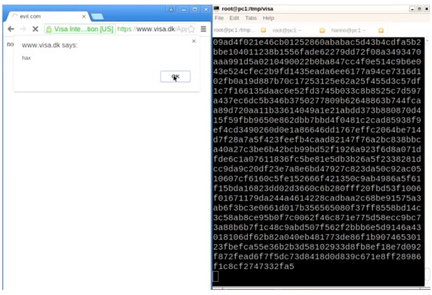
"Forbidden attack" makes dozens of HTTPS Visa sites vulnerable to tampering

Researchers say 70,000 servers belonging to others also at risk.

by **Dan Goodin** (US) - May 26, 2016 1:35pm UTC



Enlarge

Hanno Böck

Dozens of HTTPS-protected websites belonging to financial services giant Visa are vulnerable to attacks that allow hackers to inject malicious code and forged content into the browsers of visitors, an international team of researchers has found.

In all, 184 servers—some belonging to German stock exchange Deutsche Börse and Polish banking association Zwizek Banków Polskich—were also found to be vulnerable to a decade-old exploit technique cryptographers have dubbed the "forbidden attack." An additional 70,000 webservers were found to be at risk, although the work required to successfully carry out the attack might prove to be prohibitively difficult. The data came from an Internet-wide scan performed in January. Since then, Deutsche Börse has remedied the problem, but, as of Wednesday, both Visa and Zwizek Banków Polskich have allowed the vulnerability to remain and have yet to respond to any of the researchers' private disclosures.

The vulnerability stems from implementations of the transport layer security protocol that incorrectly reuse the same cryptographic nonce when data is encrypted. TLS specifications are clear that these arbitrary pieces of data should be used only once. When the same one is used more than once, it provides an opportunity to carry out the forbidden attack, which allows hackers to generate the key material used to authenticate site content. The exploit was first described in comments submitted to the National Institute of Standards and Technology. It gets its name because nonce uniqueness is a ground rule for proper crypto.

By repeating the same nonce during the TLS handshake that occurs when a browser first connects to an HTTPS-protected site, the 184 HTTPS servers violate this core tenet. That in turn makes it possible for attackers with the ability to monitor the connection—say, over an unsecured Wi-Fi network—to inject forged content into the transmission without causing the browser to detect anything is amiss.

"This results in catastrophic failure of authenticity, even if a nonce is only re-used a single time and enables us to carry out a practical forgery attack against HTTPS," the researchers wrote in a paper titled Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS. The research will also serve as the basis for a briefing scheduled in August at the Black Hat security conference in Las Vegas.

The ability for man-in-the-middle attackers to inject malicious content into HTTPS-authenticated content violates a fundamental guarantee of TLS. Attackers who are able to bypass the protection could add malicious JavaScript code or possibly add Web fields that prompt a visitor to reveal passwords, social security numbers, or other sensitive data. Although the vulnerability making the Forbidden Attack has been well documented, the new research is notable for demonstrating how it can be used against HTTPS-protected websites. Proof-of-concept attack code available online also shows that forgery attacks against visitors are practical.

A short video of the attack being used against one of the vulnerable Visa sites is here. Visa representatives didn't respond to Ars' e-mails seeking comment for this article.

Proof of concept of GCM nonce reuse attack against visa.dk

The paper—which was authored by researchers Hanno Böck, Aaron Zauner, Sean Devlin, Juraj Somorovsky, and Philipp Jovanovic—went on to warn that 70,000 HTTPS servers are potentially vulnerable to the attack because they rely on pseudo-randomly generated nonces. Given enough Web requests, there's a high probability the underlying sites would reuse one and open themselves up to an attack. The number of required requests remains extremely high, with about 2^{35} requests creating a 3-percent chance of a repeat and 2^{38} creating a 100-percent chance. As the title of the paper suggests, the Forbidden Attack works against AES-GCM, the most widely used cipher for symmetric encryption in the TLS protocol.

For the 70,000 sites identified by the researchers, an attacker would have to feed terabytes' worth of data into a Web connection to create that many requests, a requirement that probably makes the attack more theoretical than practical. Still, the risk is generally considered unacceptable for most organizations that operate HTTPS-protected sites. The researchers identified several TLS implementations that generated the pseudorandom nonces, including one in IBM's Domino Web server that was patched in March and another in load balancers from Radware, which also has been fixed.

Since the researchers carried out their scan, many of the vulnerable or potentially vulnerable sites have been fixed. But things aren't likely to meaningfully improve until engineers become more aware of the problem, and that was one of the key motivations for publishing the paper.

"I'm pretty sure if I re-scan for this issue in a year or so the number won't have changed by much," Zauner wrote in an e-mail. "Maybe there'll even be more implementations that fuck it up. No one can really tell."

This post originated on Ars Technica

READER COMMENTS 40

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY | NEWER STORY →

YOU MAY ALSO LIKE

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

The story of the *second* Soviet in space: Car crashes, curses, and carousing

The cosmonaut corps had its own cadre of cowboys.

STAY IN THE KNOW WITH

LATEST NEWS

Crime Scene Live review: Be a CSI at the Natural History Museum

Ars MacGyverica: That time we fixed a fuse box with a 6-inch nail

Can good looks save the Vauxhall Cascada from mediocrity?

Op-ed: Oracle attorney says Google's court victory might kill the GPL

"I will give you everything" promises Trump in announcing his energy plan

Building a supermassive black hole? Skip the star