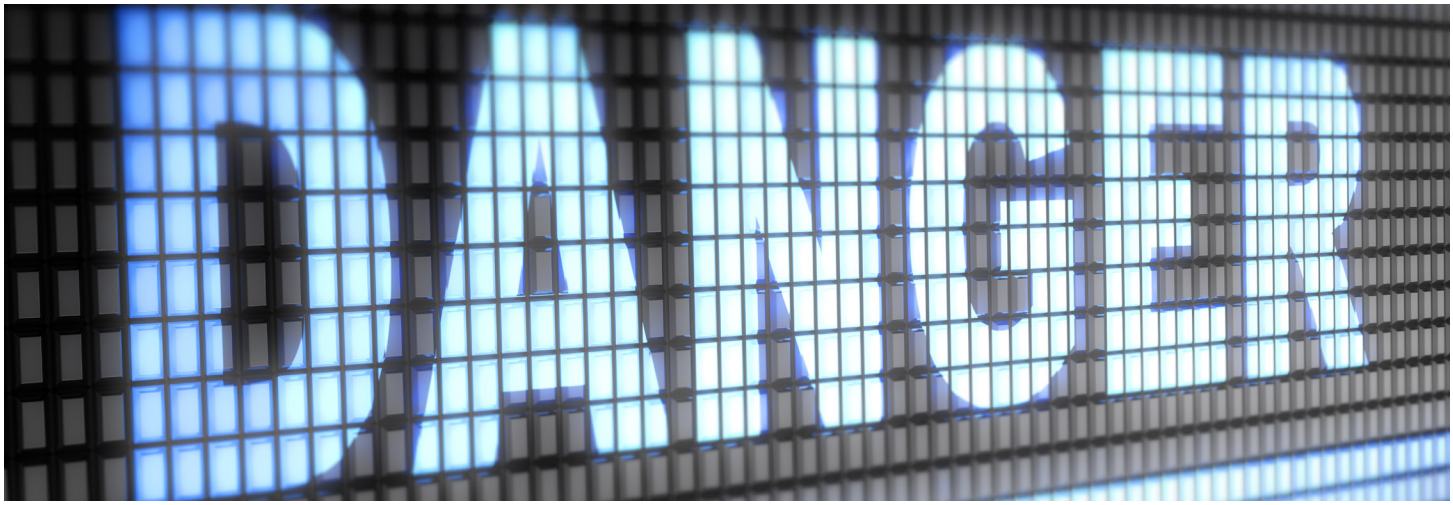


TOP TEN WAYS TO DEFEND YOUR NETWORK AGAINST THE LATEST SSL EXPLOITS

Staying on top of the latest web exploits can be a challenge for network admins who are worried about simply keeping up with all the day-to-day management tasks required by a complex environment. This article details many of the most recent popular SSL-related exploits that your network could be vulnerable to, along with simple steps you can immediately take to protect yourself.

#1 STANDARDIZE ON HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a ubiquitous protocol for secure communication over the web, allowing you to layer HTTP on top of the SSL/TLS protocol. Securing the connection provides protection against so-called Man-in-the-Middle (MITM) attacks where an attacker intercepts communications between a site and its visitor. Without the benefit of HTTPS, once the attacker has convinced the two parties that they are talking directly to each other, it becomes possible to alter the data in transit and manipulate the exchange to the attacker's benefit.

By using SSL/TLS for the entire session, HTTPS can not only encrypt the data exchanged during the secure session but also the URL request, query parameters, headers, and cookies. This heightened security makes HTTPS especially suited for high-risk interaction such as e-commerce transactions and communications over unencrypted Wi-Fi networks.

In practice, even if a site is largely configured to use HTTPS, if parts of the site are loaded via standard HTTP then it opens attack surfaces for exploit. Loading unsecured scripts or cookies, using HTTP on a login or landing page, and switching between secure and unsecure pages on a given site all become possible attack vectors for a clever hacker.

An erroneous myth is the belief that HTTPS slows website performance when, in fact, HTTPS supports Google's SPDY protocol to reduce page load latency. In any case, this imperceptible speed bump is a worthwhile trade-off for a safe online interaction. SSL Pulse reports that currently less than 20% of the Internet's most popular websites have a secure implementation of HTTPS, leaving a large majority of the web vulnerable to MITM attacks. Make sure your site isn't on the wrong side of that statistic.

#2 USE STRICT TRANSPORT SECURITY WHENEVER POSSIBLE

HTTP Strict Transport Security (HSTS) is a web security policy requiring web servers to inform web browsers that they should only interact with the server using HTTPS-protected connections. This is due to the fact that a browser has no way to know whether a plain HTTP response from a website

is because of a failure to implement SSL/TLS security, or the result of a malicious hack. An SSL-Stripping Man-in-the-Middle attack relies on converting a secure HTTPS connection into a plain HTTP connection and thereby compromising the subsequent data exchange.

The HSTS header on your website tells visiting browsers that they should only use SSL/TLS connections. One limitation is that an attacker can theoretically strip out the HSTS header on someone's first visit to a site. Some browsers circumvent this vulnerability by consulting a list for all HSTS-enabled sites, but these lists are not comprehensive, slightly limiting the protection afforded by HSTS. Another benefit HSTS provides is aiding in safeguarding your site's cookie-based login credentials that are otherwise exposed to attackers sniffing your site.

#3 256-BIT ENCRYPTION

Exhaustive key searches or "brute force attacks" are not new, but remain a viable danger to your secure network. Years ago, 40-bit keys were commonly used to encrypt data. With each bit containing either a one or a zero, that works out to over 1,000,000,000 distinct keys. The rapid growth of computational power quickly outpaced this standard and keys were lengthened to 128-bits, which allowed 340,282,366,920,938,463,463,374,607,431,768,211,456 unique encryption codes. Even this outlandish number was expected to eventually become obsolete as speeds continued to improve.

256-bit encryption has become the new standard. Provided that you are using up-to-date certificates issued by a reputable CA, your site will automatically ascertain the suitable level of encryption for a given session, based on the trade-off between speed and encryption strength supported by the client computer accessing the website.

"brute force attacks are not new, but remain a viable danger to your secure network."

#4 USE HttpOnly COOKIES

One of the underlying security mechanisms on the web is the premise of "same origin policy" wherein after trust is established with a website, permission is granted by that site to access resources on a client computer. This fact is exploited by Cross-Site Scripting (or XSS), a common security vulnerability that seeks to steal session cookies. XSS accomplishes this by injecting compromised content into the stream of data coming from the website, disguised as coming from the "same origin." This code injection gives the attacker access to information that is being shared in the connection and compromises the interaction. Using JavaScript or other scripts, malicious code can steal additional data from the client computer or otherwise wreak havoc. While XSS itself isn't new, it continues to evolve and mutate as a viable attack vector.

HttpOnly, first introduced in Microsoft Internet Explorer, is a flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when creating a cookie helps reduce the risk of client side scripts accessing the cookie by restricting the type of scripts allowed.

#5 DISABLE TLS COMPRESSION (AND "TAKE A BITE OUT OF C.R.I.M.E.")

The Transport Layer Security (TLS) protocol, the successor to the SSL protocol, includes a feature that can compress the data being exchanged between server and browser in order to reduce the bandwidth and latency issues that occasionally occur when encrypting and decrypting large amounts of data.

CRIME ("Compression Ratio Info-leak Made Easy") is a potential exploit targeting cookies over connections using the HTTPS and SPDY protocols that employ TLS data compression. An attacker can recover the content of secret authentication cookies and subsequently hijack an authenticated web session. The vulnerability is caused by a combination of plaintext injection and data leakage because of the compression. In essence, the hacker compares the size of the ciphertext sent by the browser while goading the browser into making several connections to the site. By careful examination of each exchange the attacker can deduce parts of the encrypted communication and compromise the session.

Disabling TLS compression, by either the browser or website, seals off this attack surface. While most browsers have taken steps to mitigate the danger of this exploit, site admins should ensure the security of their visitors by disabling the compression option altogether.

#6 DISABLE WEAK CIPHER SUITES

A cipher suite uses a specific combination of authentication, encryption, and algorithms to negotiate the security settings for a SSL/TLS network connection. More specifically, each cipher suite defines a key exchange algorithm, a bulk encryption algorithm, a message authentication code algorithm, and a pseudorandom function. When a TLS handshake occurs to establish a web connection, the client sends a list of the cipher suites that it supports in order of preference. The server selects a cipher suite from the list for its response and the subsequent exchange.

In 2011, security researchers developed a theoretical attack called BEAST ("Browser Exploit Against SSL/TLS") that uses a Java applet to violate same origin policy constraints and decrypt an HTTPS session between a browser and an e-commerce website. Browser vendors responded by addressing holes exploited by this attack in their latest versions. The best way that site admins can mitigate the danger from BEAST is to disable all weak cipher suites that are being recognized by their site, relying on the RC4 cipher by default.

#7 UPDATING YOUR SERVERS TO SUPPORT SECURE RENEGOTIATION

The SSL/TLS protocol has a feature called session renegotiation. This feature allows a client and server to use an existing connection to negotiate new parameters, generate new keys, and so forth, during the session. The fact that renegotiation is not directly associated with the channel creates a vulnerability that allows a third party to intercept and manipulate the data being passed between the client and the server—a classic Man-in-the-Middle attack. HTTP, SMTP, IMAP, and other protocols that rely on SSL/TLS can all be subsequently exploited. The attack initiates a renegotiation between the MITM and the server while the client is operating under the assumption that the connection is still in the initial negotiation stage.

This vulnerability led to the creation of a specific exploit known as the TLS Renegotiation Man-In-The-Middle attack (TLS Renego MITM). Many system manufacturers have released patches to fix this issue which was first discovered in 2009. However, a large percentage of sites (including prominent e-commerce websites) have still not installed the necessary patches, leaving themselves open to this attack. Not only are these sites vulnerable, but are likely to encounter connectivity issues in the future as they fall farther out of industry compliance.

A good way to protect against TLS Renego MITM is to make sure your servers support secure renegotiation. All of your servers should also be running current versions of the SSL/TLS protocol. Unfortunately, it is currently impossible for the client browser to know if a given server is still using the obsolete versions of SSL/TLS, so it becomes incumbent on IT admins to provide adequate protection for this attack surface. An alternative is to disable renegotiations altogether.

#8 CHECK YOUR SITE USING A WEB SERVER TESTER

Once you have optimized your site you still have one important step—running a SSL installation diagnostics tool, such as the free one offered by DigiCert. A good SSL test will examine installed certificates, protocol support, key exchange, and cipher strength. It can examine your SSL configuration and prescribe further steps to take to improve your overall security and eliminate attack surfaces. These tests should be run on a frequent basis to ensure that no settings have been inadvertently changed, and that ongoing updates to your site haven't broken important safeguards.

#9 STAY CURRENT WITH THIRD PARTY SECURITY UPDATES

Every network is full of third-party software fulfilling critical functions. If something isn't "broken" the tendency is not to fix it, leading to many organizations with extremely old versions of software running in their network. Clearly this can create serious holes in an otherwise well-protected environment. Attackers are routinely sniffing your network for attack surfaces left exposed by outdated software, in many cases stumbling upon vulnerabilities as they conduct scans across the entire face of the web. A poorly managed network can easily be vulnerable to dozens of potential exploits.

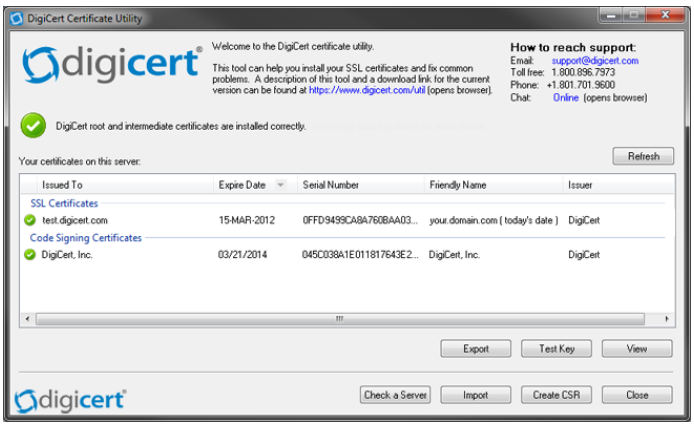
The one sure way to prevent exploits via third party software is to exercise extreme prejudice when testing and installing new software. If a piece of software isn't critically important, simply uninstall it. Once a given program has outlived its usefulness, get rid of it. Programs that you decide to keep need to be monitored as part of a regular maintenance schedule. Patch management software and version management systems can also provide important reminders when you fall behind on your updates.

#10 CONDUCT YOUR OWN PENETRATION TESTS

Even after you conduct web server testing of your external URLs, it is imperative to also conduct penetration tests (pentests) inside your network. Of particular concern is the fact that web applications running on your site often bypass your firewall, SSL encryption, and other security measures to tie straight in to your most mission-critical processes and data.

A vulnerability scanner run from inside your network can reveal many vulnerabilities that are not immediately detected by an external scan. You need to pressure test the connections between your servers and the scripts running on them to discover weak points and potential buffer overflow issues. If you are concerned about possibly disrupting production servers and important e-commerce engines then you can sometimes pentest development environments without compromising the smooth functioning and integrity of your day-to-day operations.

Cleaning up the software running on your network, especially insecure web applications, not only is important for auditing purposes, but can save you from experiencing a catastrophic attack in the very heart of your IT operations.



DigiCert Certificate Utility Tool

PICKING THE RIGHT SSL VENDOR

The Certificate Authority (CA) that you select will impact the ease-of-use, speed of issuance, uptime, OCSP/CRL latency, and a variety of features that make your network more secure and simple to manage. DigiCert® has been providing SSL Certificates and SSL management tools for nearly a decade. DigiCert assisted in developing the Extended Validation Certificate and worked in conjunction with Microsoft to develop and promote the use of Subject Alternate Names in SSL Certificates. Unlike other CAs who offer dozens or even hundreds of products unrelated to SSL encryption, creating and supporting top-shelf digital certificates is all DigiCert does. This focused energy results in better products and unmatched support.

DigiCert has an award-winning in-house technical support team and has some of the fastest certificate issuance times out of any CA—with EV certificates typically issued in a matter of hours! DigiCert doesn't outsource customer support or have phone queues. Experience the "DigiCert difference" for yourself by calling 1-855-800-3444 or visiting *www.digicert.com*.

About DigiCert, Inc.

DigiCert is a premier online trust provider of enterprise security solutions with an emphasis on authentication, PKI and high-assurance digital certificates. Headquartered in Lindon, Utah, DigiCert is trusted by a continually growing clientele of more than 60,000 of the world's leading government, finance, education and Fortune 500® organizations. DigiCert has been recognized for its excellence in customer support and the workplace, and was applauded for its value-added product features with the 2011 Frost & Sullivan Customer Value Enhancement Award for SSL Certificates.

DigiCert, Inc.
2600 West Executive Parkway Suite 500
Lehi, UT 84043 USA
+1 (801) 701-9600
www.digicert.com

©2013 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. [v0113]