Security Newsletter

14 April 2017

2017 OWASP Top 10 Release Candidate is available

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

This week the Open Web Application Security Project (OWASP) presented the first release candidate for the 2017 OWASP Top 10, the principal novelty is the presence of two new vulnerability categories: “insufficient attack detection and prevention” and “unprotected APIs.

The 2017 OWASP Top 10 misses the “unvalidated redirects and forwards,” that was the 10th item on the current list dated back 2013. The “insufficient attack detection and prevention” results from the merger of the current 4th and 7th items, “Insecure direct object references” and the “Missing Function Level Access Control.” The categories have been merged into the item “Broken access control” that was dated back in 2004.

OWASP plans to release the final OWASP Top 10 - 2017 in July or August 2017 after a public comment period ending June 30, 2017.

Read More

OWASP Top10

MS Office (former) zero-day exploited in attacks – no enabling of macros required!

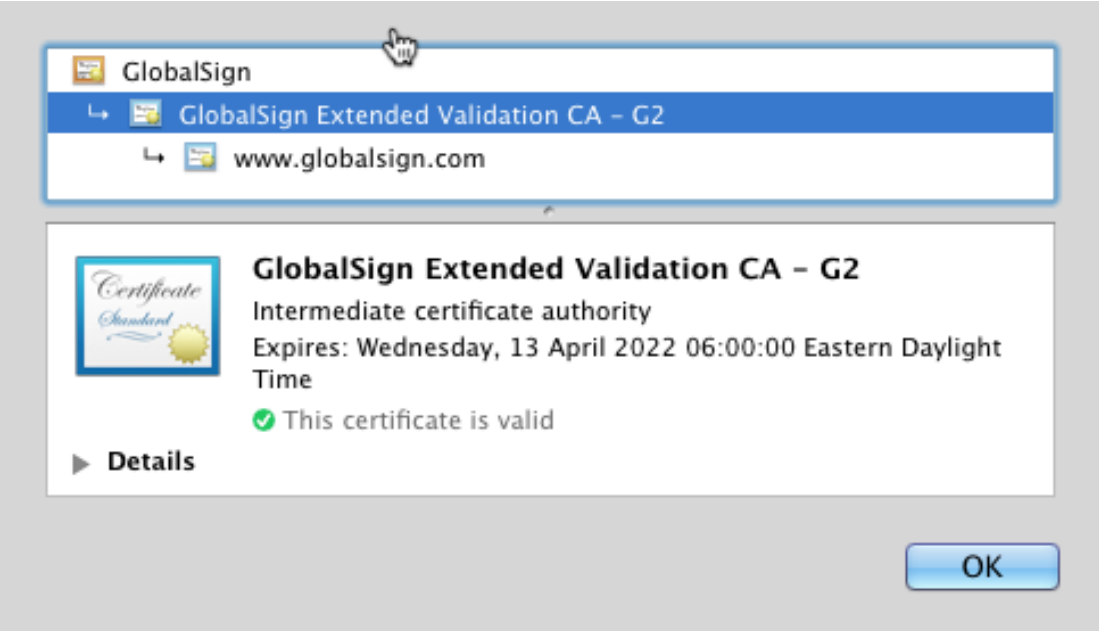
The existence of the flaw was revealed by McAfee researchers last Friday, and confirmed by FireEye researchers last Saturday. The latter shared details about it with Microsoft weeks ago, and were waiting to publicly reveal the flaw once Microsoft pushed out a patch. The patch is still to be released.

The flaw is exploited through a specially crafted Microsoft Word RTF (Rich Text Format) file, which contains an embedded OLE2link object. The object instructs Word to send a HTTP request to a remote server controlled by the attackers, to retrieve from it a malicious .hta file masquerading as a RTF file. A .hta file is an executable, and in this case it loads and executes a malicious script that closes Word (i.e. the winword.exe process), downloads additional payloads, and starts Word again and shows a decoy document. Because .hta is executable, the attacker gains full code execution on the victim's machine.

The exploit has been spotted being used to infect users with the Dridex banking malware. Microsoft has released a patch for the flaw this as part of its regular monthly Patch Tuesday. Unpatched users can protect themselves by enabling Office Protected View. Apparently, the exploit can't bypass the protection offered by that feature.

Read More

Certificate Authority Authorization



A Certificate Authority (CA) is an all powerful entity that can issue certificates for literally any domain on the planet. As the use of HTTPS, and thus certificates, is skyrocketing across the web (link)(link), we're looking to tighten up the controls on the CAs that issue them. Certificate miss-issuance, where someone else gets a certificate for your domain, is a really bad thing.

Certificate Authority Authorization (CAA) is a new mechanism that will allow site owners to specify which Certificate Authorities are authorised to issue certificates for their domain name. It's a simple DNS record so setup is a breeze and SSL Labs is now checking for it, so it's time to do it!

Right now it's optional for a CA to check for a CAA record but the CA/Browser Forum have literally just voted to make this check mandatory in the Baseline Requirements. This will land on September 8th 2017 so if you setup your record now the CAs that already check will respect it and later this year all CAs will be required to respect it.

Read More

Malware, Sir? Jenkins ‘software butler’ tool gets many security fixes

One popular and widely used toolkit for the Continuous Integration (CI) process is called Jenkins. Jenkins can not only rebuild projects after each change, but even automatically approve, sign and deploy newly-built versions into one or more test environments, and even make it flow automatically into your distribution system

The most recent Jenkins security update, for example (2017-04-10), addressed at least 32 arbitrary remote code execution bugs, both in the software itself and in many of its plugins. Bugs of this sort may sound harmless on the surface, but you can think of these holes as “metacoding” bugs, where a rogue programmer could submit perfectly legitimate code changes that would be passed as improvements, yet could at the same time sneakily subvert the build process itself. That could leave you with official software, built officially from the official source code…but with some unofficial “secret sauce” mixed in.

If you’re part of a programming team that uses Jenkins, make sure you’ve applied all needed patches, or stopped using any plugins that are now known to be vulnerable but haven’t yet been patched.

Read More

Hacker Caused Panic in Dallas by Turning ON Every Emergency Siren at Once

A hacker triggered a network of 156 emergency warning sirens for about two hours in Dallas, waking up residents and sparking fears of a disaster. The emergency warning sirens — designed to warn citizens of the Texas about dangerous weather conditions, such as severe storms and tornados — were activated around 11:40 p.m. Friday and lasted until 1:20 a.m. Saturday.

This week, Dallas city officials revealed a few details about last Friday's chaos. "It's a radio system, not a computer issue". City officials declined to provide details on how the emergency system works, noting only that "it's a tonal-type system," which suggests it could be compromised by outside radio equipment replicating the tonal code required to trigger the alarms. The whole thing sounds kind of like massive-scale phone phreaking

This is the second time when some hacker has attacked critical infrastructure in the city. Last year, some unknown hacker hacked into some traffic signals in Dallas and used them to publish jokes. For anyone who still thinks hacking always looks like a scene from Mr. Robot, the Dallas incident is just one more cautionary tale. With that in mind, it's worth remembering that not all security incidents involve Matrix-style lines of code scrolling down a computer screen. Apparently, a good old-fashioned radio hack can still wreak havoc too.

Read More

Five Inmates Built Two PCs and Hacked a Prison From Within

Five inmates from the Marion Correctional Institution (MCI) built two computers from spare parts, hid them in the ceiling of a training room closet, and used them to hack into the prison's network. Their actions were discovered in July 2015, when the prison's IT staff switched internal proxy servers, which are designed to monitor and report suspicious traffic. It immediately started reporting issues.

The five inmates managed to build their two PCs because they were part of the prison's Green Initiative program where they worked in trash management and electronics recycling. A forensic analysis of the hard drives found in the two PCs found legitimate software, hacking tools, and traces of illegal activities.

According to investigators, the inmates used these tools to capture network traffic, move laterally in the prison's network, crack passwords for active user accounts, and use these accounts to access the prison's network. They used this access to collect personal information for other inmates, apply for credit cards in the names of other inmates, and issued passes for other inmates.

Read More

Critical Security Updates from Adobe and Microsoft

Adobe and Microsoft separately issued updates on Tuesday to fix a slew of security flaws in their products. Adobe patched dozens of holes in its Flash Player, Acrobat and Reader products. Microsoft pushed fixes to address dozens of vulnerabilities in Windows and related software. Adobe pushed its own batch of security patches. The usual “critical” update for Flash Player fixes at least seven flaws. The newest version is v. 25.0.0.148 for Windows, Mac and Linux systems.

The biggest change this month for Windows users and specifically for people responsible for maintaining lots of Windows machines is that Microsoft has replaced individual security bulletins for patches with a single “Security Update Guide”. Many users are likely to be put off by the new format, which seems to require a great deal more clicking and searching than under the previous rubric.

Finally, a heads up for any Microsoft users still running Windows Vista: **This month is slated to be the last that Vista will receive security updates.** Vista was first released to consumers more than ten years ago — in January 2007 — so if you’re still using Vista it might be time to give a more modern OS a try.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.