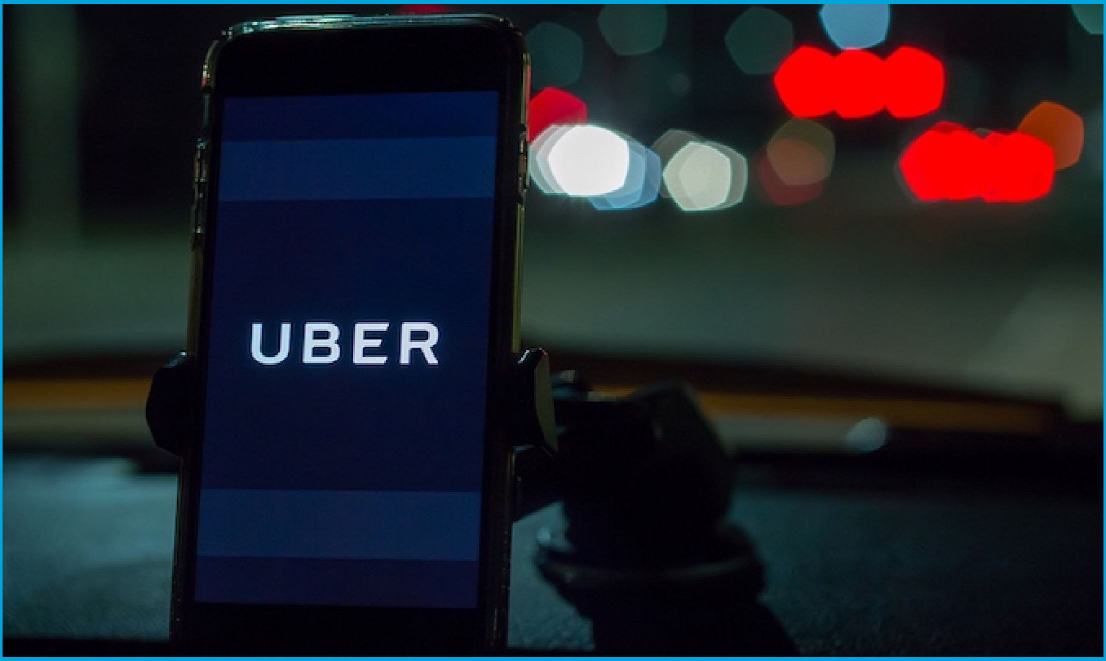
kindred

Security Newsletter

27 November 2017

Subscribe to this newsletter

Uber: Hackers stole 57m passengers, drivers' info. Uber bribed them $100k to conceal it



Uber CEO Dara Khosrowshahi posted a blog yesterday saying hackers downloaded the names and driver's license numbers of around 600,000 drivers in the United States — and some personal information of 57 million Uber users around the world. The data theft, which occurred a year ago, included names, email addresses and mobile phone numbers.

Rather than warn state and federal authorities of the personal data theft, as is required by the California upstart, Uber's chief of information security Joe Sullivan ordered that the crooks be paid off, the stolen files erased, and the whole thing hushed up, leaving riders and drivers none the wiser. The payout was disguised as a bug bounty prize complete with non-disclosure agreements signed.

It's hard to know what's most troubling about this news: The fact Uber concealed the hack for a year. That Uber forked over a hundred-grand to cyber thieves. Or that they actually believed the hackers would destroy the stolen data.

What are the consequences for users? Users may perhaps receive a lot of spam or ads on their mobile phone. Still, hackers could orchestrate phishing campaigns by creating fake Uber accounts, asking users to "confirm" their banking details or to click on links that would allow viruses into their devices.

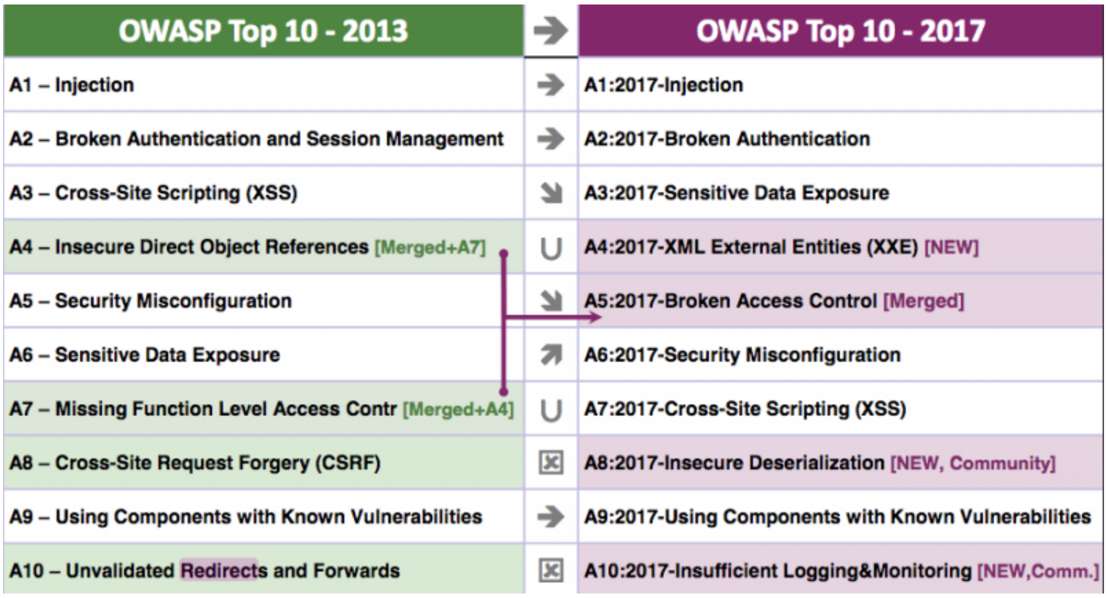
In Europe, the General Data Protection Regulation is scheduled to come into force in May 2018. Under that measure, companies that have lost personal data may be fined up to four percent of their revenues. In the case of Uber, this would be $260 million. "If they don't pay a fine, they are going to pay a cost."

Read More

Even More

Should Uber Users be Worried About Data Hack?

Final Version of 2017 OWASP Top 10 Released



OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

The final version of the 2017 OWASP Top 10 was released on Monday and some types of vulnerabilities that don't longer represent a serious risk have been replaced with issues that are more likely to pose a significant threat. One significant change compared to the 2013 OWASP Top 10 is the fact that the types of flaws that made it into the 2017 list have been selected based on the risk they pose.

The OWASP Top 10 vulnerabilities are injection, broken authentication, sensitive data exposure, XML external entity (XXE), broken access control, security misconfiguration, cross-site scripting (XSS), insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring.

API as well as web apps are covered throughout the entire Top 10. This covers mobile, single page apps, RESTful API and traditional web apps. A3:2017 Sensitive Data Exposure is now firmly about privacy and PII breaches, and not stack traces or headers. A4:2017 XXE is a new data supported item, and so tools and testers need to learn how to find and test for XXE, and developers and devops need to understand how to fix it.

A6:2017 Misconfiguration now encompasses cloud security issues, such as open buckets. A8:2017 Deserialization is a critical issue, asked for by the community. It's time to learn how to find this in tools, and for testers to understand what Java and PHP (and other serialization) looks like so it can be fixed. A10:2017 Insufficient Logging and Monitoring: Many folks think this is a missing control, rather than a weakness, but as organizations still take over half a year to detect a breach - usually from external notification - we have to fix this.

Read More

Official announcement from OWASP

Golden SAML: Newly discovered attack technique forges authentication to cloud apps

Golden SAML in a new attack vector discovered by CyberArk labs. The vector enables an attacker to create a golden SAML, which is basically a forged SAML "authentication object," and authenticate across every service that uses SAML 2.0 protocol as an SSO mechanism.

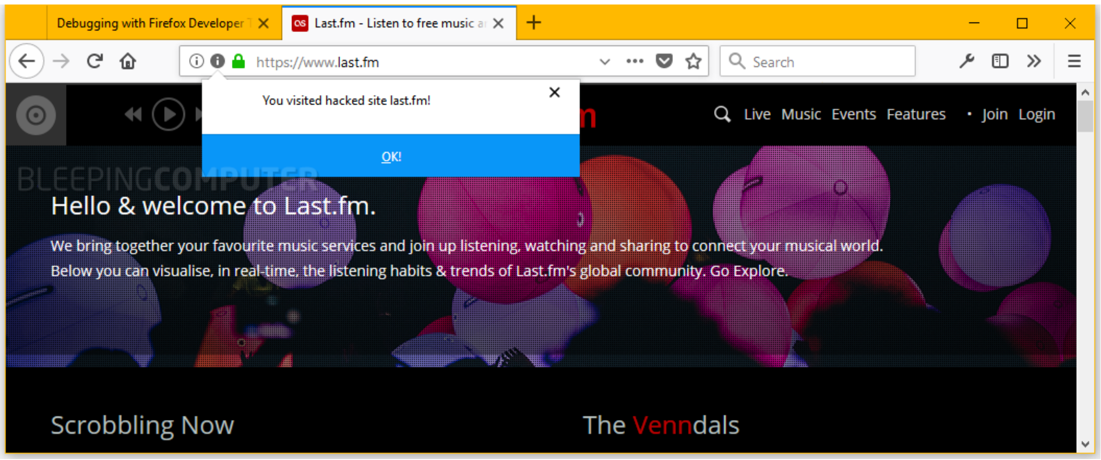
In a golden SAML attack, attackers can gain access to any application that supports SAML authentication (e.g. Azure, AWS, vSphere, etc.) with any privileges they desire and be any user on the targeted application (even one that is non-existent in the application in some cases).

In a time when more and more enterprise infrastructure is ported to the cloud, the Active Directory (AD) is no longer the highest authority for authenticating and authorizing users. AD can now be part of something bigger – a federation. A federation enables trust between different environments otherwise not related, like Microsoft AD, Azure, AWS and many others. An attacker will no longer suffice in dominating the domain controller of his victim.

The golden SAML name may remind you of another notorious attack known as golden ticket, which was introduced by Benjamin Delpy who is known for his famous attack tool called Mimikatz. The name resemblance is intended, since the attack nature is rather similar. Golden SAML introduces to a federation the advantages that golden ticket offers in a Kerberos environment – from gaining any type of access to stealthily maintaining persistency.

Read More

Firefox Will Warn Users When Visiting Sites That Suffered a Data Breach



You visited hacked site last.fm!

Hello & welcome to Last.fm.

We bring together your favourite music services and join up listening, watching and sharing to connect your musical world. Below you can visualise, in real-time, the listening habits & trends of Last.fm's global community. Go Explore.

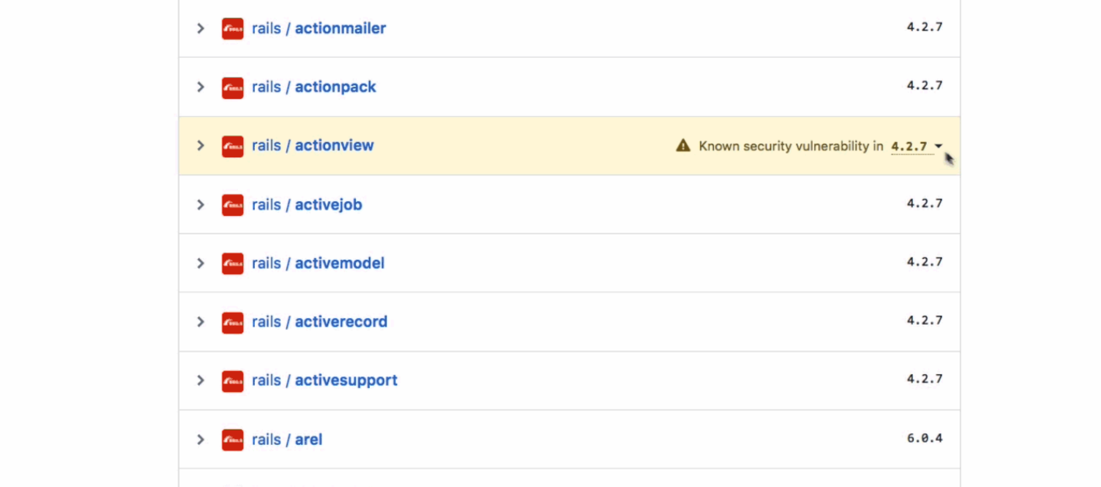
Mozilla engineers are working on a notifications system for Firefox that shows a security warning to users visiting sites that have suffered data breaches. The notifications system will use data provided by Have I Been Pwned?, a website that indexes public data breaches and allows users to search and see if their details have been compromised in any of these incidents.

The add-on is in early stages of development, and the warnings are rough on the edges. Currently, they trigger when the user visits a site included in Have I Been Pwned's list of public data breaches. The alert also includes an input field. In the add-ons current version this field doesn't do anything, but we presume it's there to allow users to search and see if their data was exposed during that site's security breach.

This new notification system will surely ruffle features with some of the breached companies. It is one thing for Have I Been Pwned to offer this kind of details on its website, buried in a corner of the Internet, but it's another thing to have news of your past breach thrust in all your site visitors' faces, especially since some of these breaches have occurred years before. One thing's for sure is that Mozilla needs to pay close attention to the language and manner it shows these notifications to users. Putting less focus on the security incident and more emphasis on encouraging users to change credentials for breached accounts is most likely the best way to go about it.

Read More

Introducing security alerts on GitHub



rails / actionmailer	4.2.7
rails / actionpack	4.2.7
rails / actionview	Known security vulnerability in 4.2.7
rails / activejob	4.2.7
rails / activemodel	4.2.7
rails / activerecord	4.2.7
rails / activesupport	4.2.7
rails / arel	6.0.4

Code hosting service GitHub now warns developers if certain software libraries used by their projects contain any known vulnerabilities and provides advice on how to address the issue. The new security feature added by GitHub is designed to alert developers when one of their project's dependencies has known flaws. The Dependency graph and the security alerts feature have been automatically enabled for public repositories, but they are opt-in for private repositories.

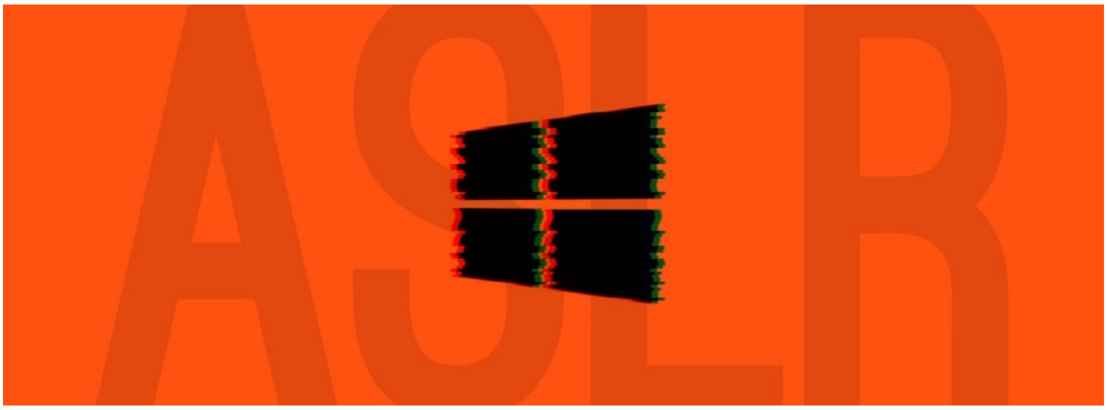
When a vulnerable library is detected, a "Known security vulnerability" alert will be displayed next to it in the Dependency graph. Administrators can also configure email alerts, web notifications, and warnings via the user interface, and they can add the teams or individuals who should see the alerts.

The information provided to administrators includes the type of flaw, its severity, and affected versions. There is also a link that points to a page where additional details are available. GitHub currently tracks vulnerabilities that have been assigned a CVE identifier, but since many publicly disclosed flaws don't have CVEs, the company will also try to warn users of issues that don't have one. "We'll continue to get better at identifying vulnerabilities as our security data grows," GitHub said.

Read More

GitHub Warns Developers When Using Vulnerable Libraries

Windows 8 and later fail to properly apply ASLR?



Windows 8, Windows 8.1, and subsequent Windows 10 variations fail to properly apply ASLR in some use cases, rendering this crucial Windows security feature useless. Address Space Layout Randomization (ASLR) is a computer security technique that randomizes the memory address where application code is executed.

While looking into a recently disclosed 17-years-old vulnerability affecting the Microsoft Office equation editor, CERT/CC vulnerability analyst Will Dormann discovered that ASLR was not randomizing the memory code locations of application binaries in specific conditions. According to Dormann, when users turned on system-wide ASLR protection, a bug in the feature's implementation on Windows 8 and later would not generate enough entropy (random data) to start application binaries in random memory locations. This is the equivalent of ASLR not being enabled at all.

Redmond's response, posted here, was that ASLR is working as intended, and that the lack of randomisation discovered by Will Dormann - with assistance from Matt Miller of Microsoft - was a feature, not a bug. users must enable ASLR in a system-wide bottom-up configuration in order for ASLR to work properly. While Microsoft is expected to fix the issue in a future patch, currently, the only way of starting ASLR in the proper configuration is by tinkering with the Windows Registry.

Read More

Microsoft says Win 8/10's weak randomisation is 'working as intended'

Microsoft: Clarifying the behavior of mandatory ASLR

KeePass – a password manager that's cloud-less (but complex)

It can get a bit overwhelming for the average person to understand all the security-related best practices they might hear about online or at work. This one is certainly worth harping on about though: credential reuse. Using that same easy-to-type password on every website and service you use practically rolls out the red carpet for an attacker into your online life. So if there's one thing we suggest to everyone that will go a long way to improve their overall security, it's using a password manager.

KeePass is an open-source password manager that does all the things you'd expect a password manager to do at the very least – it stores all websites and service credentials in a highly-encrypted vault that can only be unlocked with one Master Password, which becomes the only password you need to remember.

But a key difference between KeePass and cloud-based password managers is that KeePass is software you run locally – not an online service – and your KeePass vault is something you store in a location of your choosing. That can be on a hard drive, a portable USB key, or even a cloud service you subscribe to. It's up to you where your password vault goes and who has access to it.

Read More

Enpass: An alternative to Keypass

Cutting room floor

- Kali Linux 2017.3 Release
- A penetration tester's guide to sub-domain enumeration
- Proactive Malicious Domain Search
- A Sheep in Wolf's Clothing – Finding RCE in HP's Printer Fleet
- From Markdown to RCE in Atom
- Google Collects Android Location Data Even When Location Service Is Disabled
- DOMPurify: DOM-only, fast, tolerant XSS sanitizer for HTML, MathML and SVG.
- Chromebook exploit earns researcher second $100k bounty
- Android Flaw Lets Attackers Capture Screen and Record Audio
- Another Tor browser feature makes it into Firefox first party isolation
- ID card security: Spain is facing chaos over chip crypto flaws
- Samba needs two patches, unless you're happy for SMB servers to dance for evildoers
- F5 Crypto Fail: BIG-IP SSL vulnerability CVE-2017-6168
- Apple's Latest MacOS Security Update Contained Fix for Plug-n-Hack USB Attack
- Honey Accounts
- NIST SP800-190: Application Container Security Guide

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.

You can access the previous newsletters at https://news.infosecgur.us