Top 10 Security Breaches of 2017 – and What To Do

Author: Veerendra G

Introduction

Security attacks and breaches happen routinely, costing companies millions of dollars, along with a decline in their reputation and the public's trust in them. Attackers are constantly innovating on the different methods and paths to infiltrate networks and steal confidential information. Major data breaches occur because companies fail to patch critical vulnerabilities in time.

A data breach incident leads to confidential data being viewed, stolen or blocked by an unauthorized person or group. Often, this confidential information contains personal information, contractual business documents, government documents, etc., which attackers use to make money for personal gain, or to damage a company's reputation, etc.

This article highlights the latest 10 security attacks and breaches that exploited known vulnerabilities in software; and highlights what we could learn from it.

01. Equifax Data Breach

Equifax, a consumer credit reporting agency, suffered a distressing security breach where the personal and financial information of 145.5 million consumers was exposed, including the date of birth, SSN, Driver's License number and address, etc. This was one of the biggest *potential* identity theft scares in recent times.

Equifax revealed that attackers exploited a vulnerability in **Apache Struts (CVE-2017-5638),** a widely used enterprise platform. This vulnerability had been reported in March 2017, and a patch to solve this vulnerability had been available with simple and clear instructions. Equifax was breached in mid of May; it discovered the breach end of July; and it revealed the crisis to the public in September, a month later.

The vulnerability **(CVE-2017-5638)** was in the Jakarta Multipart parser in Apache Struts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header; the March 2017 attackers exploited the vulnerability with a Content-Type header containing a #cmd= string.

02. SEC Data Breach

In September 2017, the **U.S. Securities and Exchange Commission (SEC)** admitted that hackers had breached EDGAR, its corporate filing system in 2016. The SEC's EDGAR corporate filing system is the hub of financial information, and contains non-public sensitive information. Attackers' may have used this information to gain an advantage in stock trading, and definitely had the power to change the market.

The breach was discovered during an audit in October 2016, along with the knowledge that the staff has been using private, unsecured email accounts to exchange confidential information.

Attackers exploited a software vulnerability in the test filing component of the EDGAR system, where companies submit their financial filings. According to the SEC Chairman Jay Clayton, the vulnerability was patched promptly after the discovery and an investigation initiated to understand the breach.

03. Massive Data Breach Hits 6000 Indian Enterprises

In October 2017, **Seqrite Cyber Intelligence Labs** and its partner **seQtree InfoServices** tracked an advertisement on the **DarkNet** that offers access to the servers and database dump of over 6000 Indian enterprises, including government organizations, internet service providers, banks, and businesses.

The unidentified hacker has priced the information at **15 Bitcoins** (approximately 41.89 lakh rupees) with an offer to take down the network of affected organizations for an unspecified amount. Along with access, the hacker is also selling credentials, PII, and various contractual business documents, and claims to have access to a large database of Asia Pacific Network Information Centre (APNIC).

The hackers also claimed to have the ability to manipulate the IP address allocation pool, which could trigger a serious outage or Denial of Service attack-like condition, said the IANS report.

“This could impact various content delivery network (CDN) and hosting providers as well. If the hacker gets an interested buyer, then an attack on the system could disrupt Internet IP allocation and affect Internet services in India," Seqrite said.

Prashant Pandey, founder and chief knowledge officer at **Kratikal Tech**, offers a theory on how the breach occurred. "It is a logical conjecture that the attacker used the same vulnerability **in Apache Struts (CVE-2017-5638)** as was exploited using the Equifax hack. Simply put, arbitrary booby-trapped Java codes can be passed as XML objects to the Struts, resulting in unprecedented responses. This might have resulted in the data breach. Still, this is the best guess."

04. Massive WannaCry Ransomware Attack

A ransomware attack called **WannaCry 2.0** hit computers in 99 countries in May 2017, including the Russian Interior Ministry, UK Hospitals, Chinese universities, Hungarian telecoms, and FedEx branches. Also referenced as **WCry**, **WanaCrypt0r, WannaCrypt**, this ransomware encrypted data; and demanded bitcoins in exchange for a decryption key.

The attackers used **EternalBlue (CVE-2017-0144)**, a publically disclosed vulnerability in Microsoft Windows systems, to create a ransomware with worm capabilities, which leveraged **SMB exploit** to spread to other Windows endpoints once inside a network.

Microsoft has released a patch **MS17-010** in March to address this vulnerability, even for the Windows XP operating system, which had reached EOL in April 2014, but many institutions hadn't applied it and were therefore vulnerable to the WannaCry ransomware.

05. Petya Ransomware Attack

Yet another ransomware attack with worm capabilities began spreading across Europe by end of June 2017. Massive in scale, Petya, also referenced as NonPetya, crippled computers in 64 countries around the world, including Belgium, Brazil, Germany, Russia, and the United States. Similar to Wannacry, it encrypted the data and demanded its ransom in bitcoins for a decryption key.

As per Microsoft, “the malware was initially delivered via Ukrainian company's (M.E.doc) update service for their finance application, which is popular in Ukraine and Russia”. After the initial infection, it attempted to spread across networks using the SMB protocol by exploiting **EternalBlue** **(CVE-2017-0144)** and **CVE-2017-0145** vulnerabilities.

Microsoft released patch **MS17-010** to address these vulnerabilities, even for the Windows XP operating system, which had reached EOL in April 2014, but not everyone had installed the patch.

06. Ransomware Attack Cuts Access to X-Rays at Surgery Center

An Arkansas-based surgery center was hit by ransomware in July 26, 2017, which shut down access to electronic patient data and also impacted imaging files, including X-rays. This incident, listed by the HIPAA Breach Reporting Tool website as a hacking/IT incident, involved a network server and affected 128,000 individuals.

The notice posted by the Arkansas Oral & Facial Surgery Center stated that, "…the ransomware had been installed on our systems by an unauthorized individual at some point earlier that morning or the evening before." And "the motivation behind this incident was extortion, and not the theft of patient information. We have notified the FBI of this incident."

The Department of Homeland Security in August 2017, issued an alert about vulnerabilities in certain **Siemens medical imaging products running Windows 7** that could enable hackers to "remotely execute arbitrary code." Medical device expert Billy Rios calls those issues "exactly the types of vulnerabilities targeted by ransomware."

07. ABTA Data Breach

Association of British Travel Agents (ABTA) is the UK's largest travel association, representing travel agents and tour operators. ABTA was breached on 27 February 2017; the personal information of 650 ABTA members and 43,000 consumers was exposed. Approximately 1,000 files of personal identity data were taken and email addresses and encrypted passwords of registered customers and members were also stolen.

On immediate investigation, ABTA identified that its own systems remained secure and the vulnerability was in the web server for abta.com, managed by a third-party web developer and hosting company. ABTA CEO Mark Tanzer said that a hacker used the vulnerability in the firm's web server to access the data provided by its members and some of those members' customers.

08. ESEA Data Breach

The database of E-Sports Entertainment Association (ESEA), one of the largest competitive video gaming community, was breached in December 2016. The profiles of 1.5 million players was exposed to hackers, which included personal information such as usernames, emails, private messages, IPs, mobile phone numbers, forum posts, hashed passwords, and hashed secret question answers.

An ESEA spokesperson confirmed that the breach was part of an extortion demand. The attacker contacted the company through its bug bounty program on December 27 and told the company that if it didn't pay $100,000, the data would either be sold or released. However, ESEA refused to give in to the attackers' demands and contacted the authorities.

ESEA worked to identify the source of the vulnerability and have taken the appropriate action to patch the vulnerability. ESEA also said they will continue to work with both our developers and independent security experts to improve security and invest in strengthening ESEA's infrastructure.

09. Mail.ru Forum Data Breach

In August 2016, hackers were able to obtain roughly 25 million username and password combinations from three different sub domains of Mail.ru, cifre.mail.ru, parapa.mail.ru and tanks.mail.ru. These affected sub domain host forums for games acquired by Mail.Ru. As per Leaked Source team “Not a single website used proper password storage, they all used some variation of MD5 with or without unique salts”. This allowed hackers to crack over 15 million passwords from the various forums.

The affected domain was running the vBulletins forum; attackers exploited the SQL injection vulnerability in the older vBulletin forum application to gain access to the database.

10. Ubuntu Forum Data Breach

Ubuntu online forums were hacked in July 2016. On 14th July 2016, Canonical’s IS team were notified by a member of the Ubuntu Forums Council that someone was claiming to have a copy of the Forums database. After some initial investigation, we were able to confirm there had been an exposure of data. Attackers used a known SQL injection vulnerability in the Forum runner add-on, which had not yet been patched.

The information of 2 million users had been exposed to hackers, which included IP addresses, usernames, email IDs. The forum was shut down as a precaution and all system and database passwords were reset.

Conclusion

A common thread in the above data breaches is the exploitation of a known vulnerability in the software which was not patched on time. Vulnerabilities or security bugs in an application were exploited to get control of the systems to cause damage, or access authorized information etc. for personal profit.

All the above breaches could have been avoided by applying the security patches as soon as they were available. The Equifax data breach could have been completely avoided if Equifax had patched the vulnerability (**CVE-2017-5638**) within a month from the patch available date. Less than a month is sufficient to test and roll out the patch to the production servers for such critical vulnerabilities.

About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. SecPod's deep information security expertise exceptionally positions the company to help solve complex endpoint security challenges. Headquartered in Bangalore with operations in USA, SecPod's products are deployed across diversified verticals.

Contact Us

Web: www.secpod.com Tel: +91-80-4121 4020
Email: info@secpod.com +1-918-625-3023