Security Newsletter

27 August 2018

Subscribe to this newsletter

Primer on two-factor authentication

Many online accounts allow you to supplement your password with a second form of identification, which can prevent some prevalent attacks. The second factors you can use to identify yourself include authenticator apps on your phone, which generate codes that change every 30 seconds, and security keys, small pieces of hardware similar in size and shape to USB drives.

Since innovations that can actually improve the security of your online accounts are rare, there has been a great deal of well-deserved enthusiasm for two-factor authentication (as well as for password managers, which make it easy to use a different random password for every one of your online accounts.) These are technologies more people should be using.

However, in trying to persuade users to adopt second factors, advocates sometimes forget to disclose that all security measures have trade-offs. Before you require a second factor to login to your accounts, you should understand the risks, have a recovery plan for when you lose your second factor(s), and know the tricks attackers may use to defeat two-factor authentication.

Read More

Common services supporting 2FA

Experts Urge Rapid Patching of ‘Struts’ Bug

In September 2017, Equifax disclosed that a failure to patch one of its Internet servers against a pervasive software flaw — in a Web component known as Apache Struts — led to a breach that exposed personal data on 147 million Americans. Now security experts are warning that blueprints showing malicious hackers how to exploit a newly-discovered Apache Struts bug are available online, leaving countless organizations in a rush to apply new updates and plug the security hole before attackers can use it to wriggle inside.

On Aug. 22, the Apache Software Foundation released software updates to fix a critical vulnerability in Apache Struts, a Web application platform used by an estimated 65 percent of Fortune 100 companies. Unfortunately, computer code that can be used to exploit the bug has since been posted online, meaning bad guys now have precise instructions on how to break into vulnerable, unpatched servers.

“Critical remote code execution vulnerabilities like the one that affected Equifax and the one we announced today are incredibly dangerous for several reasons: Struts is used for publicly-accessible customer-facing websites, vulnerable systems are easily identified, and the flaw is easy to exploit,” wrote Semmle co-founder Pavel Avgustinov. “A hacker can find their way in within minutes, and exfiltrate data or stage further attacks from the compromised system. It’s crucially important to update affected systems immediately; to wait is to take an irresponsible risk.”

The vulnerability affects all supported versions of Struts 2. Users of Struts 2.3 should upgrade to version 2.3.35; users of Struts 2.5 should upgrade to 2.5.17.

Read More

Even More

No Patch Available Yet for New Major Vulnerability in Ghostscript Interpreter

Tavis Ormandy, a Google Project Zero security researcher, has revealed details about a new major vulnerability discovered in Ghostscript, an interpreter for Adobe's PostScript and PDF page description languages. Ghostscript is by far the most widely used solution of its kind. The Ghostscript interpreter is embedded in hundreds of software suites and coding libraries that allow desktop software and web servers to handle PostScript and PDF-based documents. For example, you'll find Ghostscript inside ImageMagick, Evince, GIMP, and all PDF editing or viewing software.

Exploiting the bug Ormandy discovered requires that an attacker sends a malformed PostScript, PDF, EPS, or XPS file to a victim. Once the file reaches the Ghostscript interpreter, the malicious code contained within will execute an attacker's desired on that machine.

At the time of writing, there is no fix available. "I *strongly* suggest that [Linux] distributions start disabling PS, EPS, PDF and XPS coders in [ImageMagick's] policy.xml by default," Ormandy said.

Read More

Even More

Cutting room floor

- Adobe Issues Emergency Patches for Critical Flaws in Photoshop CC
- Supply Chain Attack Hits Organizations In South Korea
- Alleged SIM Swapper Arrested in California
- Mitre ATT&CK™ and the FIN7 Indictment: Lessons for Organizations
- Windows 10 alert: All versions get new Intel patches for Spectre, Foreshadow bugs
- Hacker holds the data of 20,000 Superdrug customers to ransom
- TLS Certs Outliving Domain Ownership Open Door to MitM and DoS
- Cloud Product Accidentally Exposes Users' TLS Certificate Private Keys
- New Attack Recovers RSA Encryption Keys from EM Waves Within Seconds
- Cloudflare's approach to protect from cache poisoning
- Dark Tequila Banking Malware Uncovered After 5 Years of Activity
- What are Amazon Zelkova and Tiros? AWS looks to reduce S3 configuration errors
- Skype's End-to-End Encryption Goes Live
- New "Turning Tables" Technique Bypasses All Windows Kernel Mitigations
- Gmail's Confidential Mode Lets You Send Self-Destructing Emails...beware of Phishing attempts
- Fake Android Fortnite version circulating on the web to spread malware

#Tech and #Tools

- Singularity: A DNS rebinding attack framework
- CVE-2018-11776: How to find 5 RCEs in Apache Struts with Semmle QL
- Burp Suite 2.0 beta now available
- Enumerating registered BlackHat attendees with the BCard API
- CrowdStrike Adds Malware Search Engine to 'Hybrid Analysis'
- Serious Security: How to stop dodgy HTTP headers clogging your website
- Security Concerns Surrounding WebAuthn: Don't Implement ECDAA (Yet)
- DNS Rebinding Headless Browsers
- More Ghostscript Issues: Should we disable PS coders in policy.xml by default?
- Pacu: The Open Source AWS Exploitation Framework
- Useless CSP
- Peeking Behind the Curtains of Serverless Platforms
- Account takeover due to blind MongoDB injection in password reset

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