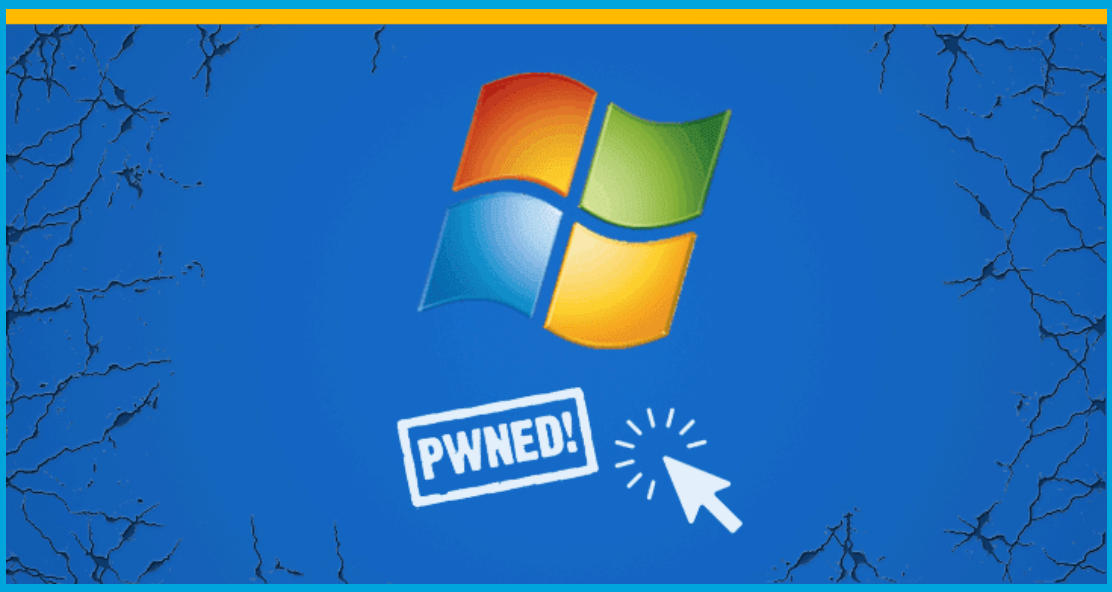
kindred

# Security Newsletter

16 April 2018

Subscribe to this newsletter

# Warning: Your Windows PC Can Get Hacked by Just Visiting a Site




Can you get hacked just by clicking on a malicious link or opening a website? — YES.

Microsoft has just released its April month's Patch Tuesday security updates, which addresses multiple critical vulnerabilities in its Windows operating systems and other products, five of which could allow an attacker to hack your computer by just tricking you visit a website.

An attacker can exploit these issues by tricking an unsuspecting user to open a malicious file or a specially crafted website with the malicious font, which if open in a web browser, would hand over control of the affected system to the attacker.

Windows Microsoft Graphics is also affected by a denial of service vulnerability that could allow an attacker to cause a targeted system to stop responding. This flaw exists in the way Windows handles objects in memory. Besides this, Microsoft has also patched multiple remote code execution vulnerabilities in Microsoft Office and Microsoft Excel, which could allow attackers to take control of the targeted systems.

The security updates also include patches for six flaws in Adobe Flash Player, three of which were rated critical.

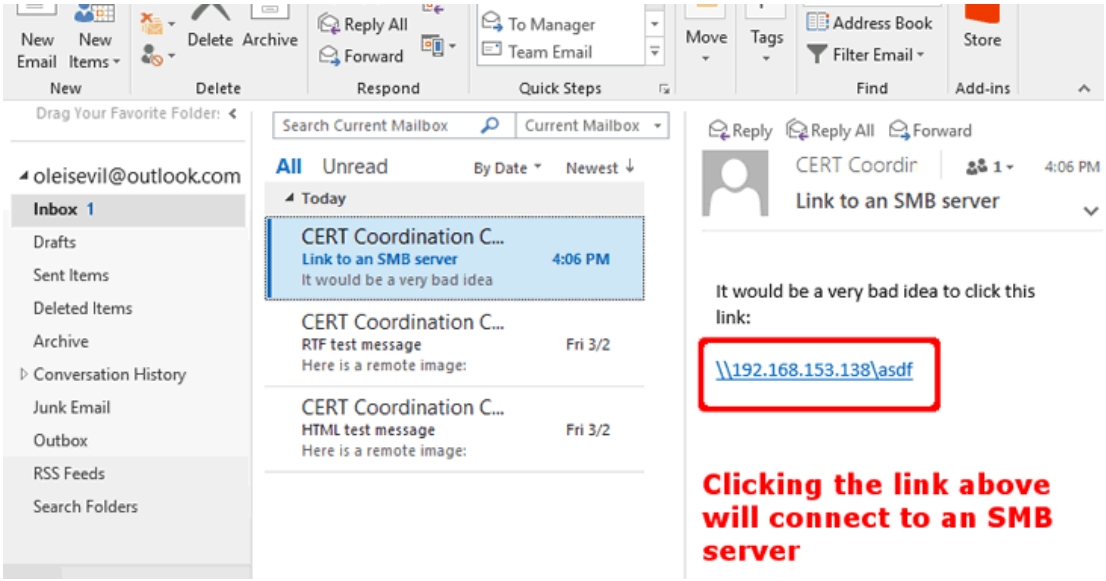
Users are strongly advised to apply security patches as soon as possible to keep hackers and cybercriminals away from taking control of their computers.

Read More

Microsoft's April 2018 Patch – 65 vulns, 24 critical

CVE-2018-1013 Advisory

# Flaw in Microsoft Outlook Lets Hackers Easily Steal Your Windows Password




A security researcher has disclosed details of an important vulnerability in Microsoft Outlook for which the company released an incomplete patch this month—almost 18 months after receiving the responsible disclosure report.

The Microsoft Outlook vulnerability (CVE-2018-0950) could allow attackers to steal sensitive information, including users' Windows login credentials, just by convincing victims to preview an email with Microsoft Outlook, without requiring any additional user interaction.

If you have already installed the latest Microsoft patch update, that's great, but attackers can still exploit this vulnerability. So, Windows users, especially network administrators at corporates, are advised to follow the below-mentioned steps to mitigate this vulnerability. Block specific ports (445/tcp, 137/tcp, 139/tcp, along with 137/udp and 139/udp) used for incoming and outgoing SMB sessions. Block NT LAN Manager (NTLM) Single Sign-on (SSO) authentication. Always use complex passwords, that cannot be cracked easily even if their hashes are stolen (you can use password managers to handle this task). Most important, don't click on suspicious links provided in emails.

Read More

# Practical passwordless authentication comes a step closer with WebAuthn


Three major browser makers —Google, Microsoft, and Mozilla—have put their official backing behind a new W3C API called Web Authentication (WebAuthn) that is advertised as a reliable alternative to passwordless online authentication.

WebAuthn is a specification to allow browsers to expose hardware authentication devices—USB, Bluetooth, or NFC—to sites on the Web. These hardware devices enable users to prove their identity to sites without requiring usernames and passwords. The spec has been developed as a joint effort between FIDO, an industry body that's developing secure authentication systems, and W3C, the industry group that oversees development of Web standards.

With WebAuthn-enabled browsers and sites, users can sign in using both integrated biometric hardware (such as the fingerprint and facial-recognition systems that are widely deployed) and external authentication systems such as the popular YubiKey USB hardware. With WebAuthn, no user credentials ever leave the browser and no passwords are used, providing strong protection against phishing, man-in-the-middle attacks, and replay attacks.

With WebAuthn in place, widespread adoption of passwordless authentication will be much more practical. We're certainly not going to see the end of the password overnight, but this is the kind of infrastructure that needs to be in place before it can credibly be replaced.

Read More

Even More

## #Facebook

- Facebook's Zukerberg Quietly Drops Another Privacy Bomb - Facial Recognition
- How to Find Out Everything Facebook Knows About You
- Facebook Offering $40,000 Bounty If You Find Evidence Of Data Leaks
- These are Mark Zuckerberg's notes from his testimony to Congress
- It's weirdly hard to steal Mark Zuckerberg's trash
- Congress grills Facebook CEO over data misuse – as it happened
- Facebook data analyzer tool

## Cutting room floor

- Don't Give Away Historic Details About Yourself
- 3 critical Flash vulnerabilities patched. Update now!
- SirenJack: Hackers can hijack emergency alert sirens with a $35 radio and laptop
- Exploitation of Drupalgeddon2 Flaw Starts After Publication of PoC Code
- Thai mobile operator spills 46k people's data due to S3 bucket leak
- Avoiding Holes in Your AWS Buckets
- Security Headers is changing domain and branding
- Gmail is secure. Netflix is secure. Together they're a phishing threat
- Serverless Architectures: A Paradigm Shift in Application Security
- Over 65,000 Home Routers Are Proxying Bad Traffic for Botnets, APTs
- Researchers Catch Android OEMs Lying About Security Patches
- Oblivious DNS could protect your internet traffic against snooping

## #Tech and #Tools

- Securing DNS across all of my devices with Pi-Hole + DNS-over-HTTPS + 1.1.1.1
- OpenSnitch is a GNU/Linux port of the Little Snitch application firewall.
- P4wnP1: Customizable USB attack platform on a low cost Raspberry Pi Zero
- Drupwn: Yet another Drupal scanner
- Remote Hash Extraction On Demand Via Host Security Descriptor Modification
- Creating custom YARA rules
- CyberArk Password Vault Web Access Remote Code Execution
- Hackers Found Using A New Code Injection Technique to Evade Detection
- Signal Bypass Screen locker
- Compromising OpenDrive's Cloud Storage Accounts – Or How Not to Design Session Management
- DomLink—Automating domain discovery
- https://blog.grimm-co.com/post/heap-overflow-in-the-necp_client_action-syscall/
- XSS in pastebin.com via unsanitized markdown output
- Snallygaster - a Tool to Scan for Secrets on Web Servers
- Spectrum: Extending Cloudflare To 65,533 More Ports

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.