

Contents

01 Patches Notes

- WordPress security plugin Hide My WP addresses SQL injection, deactivation flaws
- Patch Apache HTTP Server Vulnerability getting Exploited
- New Windows 10 zero-day gives admin rights, gets unofficial patch

02 Cyber Attack

- 2.1 million People Affected by Breach at DNA Testing Company
- Panasonic Suffers Data Breach After Hackers Hack into Its Network
- Ransomware Gang threatens to leak 1.5TB of Supernus Pharmaceuticals Data

03 Malware and Vulnerabilities

- Over 300,000 Android users have downloaded banking trojan
- 8-year-old HP printer vulnerability affects 150 printer models
- CronRAT: A New Linux Malware That's Scheduled to Run on February 31st

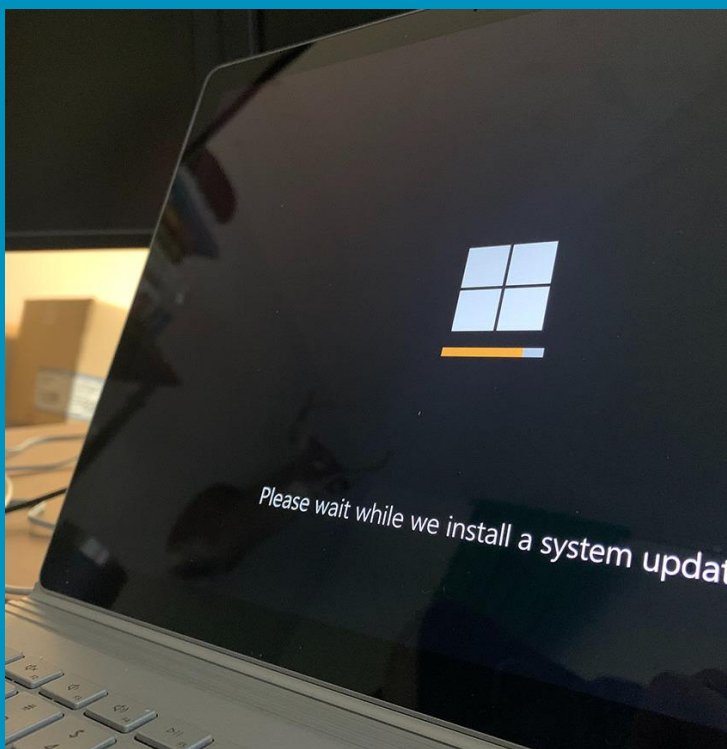
04 AWS re: Invent Recap

- Amazon launches preview of new AWS Private 5G managed service
- AWS introduces IoT TwinMaker, a new service to easily create digital twins
- AWS Re:invent Major Announcements

Patches Notes

PATCH APACHE HTTP SERVER VULNERABILITY GETTING EXPLOITED

- After it was discovered that a newly patched vulnerability had been used in attacks, organisations are being encouraged to ensure that their Apache HTTP servers are up to date.
- CVE-2021-40438 is a server-side request forgery (SSRF) vulnerability that may be exploited against httpd web servers with the mod proxy module installed. An attacker can take advantage of this serious weakness by sending a properly crafted request to the module, which will cause the request to be forwarded to an arbitrary origin server. [↗](#)



WORDPRESS SECURITY PLUGIN HIDE MY WP ADDRESSES SQL INJECTION, DEACTIVATION FLAWS

- A severe SQL injection (SQLi) vulnerability and a security vulnerability in Hide My WP, a popular WordPress security plugin, allowed unauthenticated attackers to deactivate the software.
- Now patched, the bugs were discovered during an audit of several plugins on a customer's website by Dave Jong, CTO of Patchstack, which protects WordPress websites from vulnerabilities and runs a WordPress-focused bug hunting platform. [↗](#)

NEW WINDOWS 10 ZERO-DAY GIVES ADMIN RIGHTS, GETS UNOFFICIAL PATCH

- A free unofficial patch has been issued to protect Windows users from a zero-day vulnerability in the Mobile Device Management Service that affects Windows 10, version 1809 and later.
- The security issue is hidden in the "Access work or school" settings, and it works around a Microsoft patch released in February to fix an information leak bug identified as CVE-2021-24084. [↗](#)

2.1 Million People Affected by Breach at DNA Testing Company

- DNA Diagnostics Center (DDC), an Ohio-based DNA testing company, announced a data breach impacting 2.1 million persons this week.
- DDC claimed it discovered unauthorised access to its network on August 6 in a data breach report posted on its website. The intruders had accessed an archived database, according to the inquiry. [↗](#)

CYBER ATTACKS



PANASONIC SUFFERS DATA BREACH AFTER HACKERS HACK INTO ITS NETWORK

- Panasonic, a Japanese consumer electronics company, has revealed a security incident in which an unauthorised third-party gained access to its network and might accessed data from one of its file servers.
- "It was found, as a consequence of an internal investigation, that certain data on a file server had been accessed during the attack," the company said in a brief statement released on November 26. [↗](#)



RANSOMWARE GANG THREATENS TO LEAK 1.5TB OF SUPERNUS PHARMACEUTICALS DATA

- Supernus Pharmaceuticals, a biopharmaceutical business, reported last week that it had been the victim of a ransomware attack that resulted in a considerable amount of data being exfiltrated from its network.
- It happened in mid-November, according to Supernus, when a ransomware gang acquired data on select systems, installed malware to limit access to files, and then threatened to disclose the exfiltrated data. [↗](#)



Malware and Vulnerabilities




OVER 300,000 ANDROID USERS HAVE DOWNLOADED BANKING TROJAN


- After falling victim to malware that evaded detection by the Google Play app store, over 300,000 Android smartphone users downloaded what turned out to be banking trojans.
- Malicious versions of regularly downloaded software, such as document scanners, QR code readers, fitness trackers, and cryptocurrency apps,



8-YEAR-OLD HP PRINTER VULNERABILITY AFFECTS 150 PRINTER MODELS

- An attacker might leverage the flaws to execute a 'cross-site printing' attack, but a user on the susceptible printer's network would have to be duped into visiting a malicious website first.
- If successful, the website might remotely print a document on the susceptible printer using a maliciously designed typeface, allowing the attacker to execute code on the device. 

CRONRAT: A NEW LINUX MALWARE THAT'S SCHEDULED TO RUN ON FEBRUARY 31ST

- Researchers have discovered a novel Linux remote access trojan (RAT) that uses a never-before-seen stealth approach that includes scheduling malicious actions for execution on February 31st, a non-existent calendar day.
- CronRAT is a cunning trojan that "allows server-side Magecart data theft while avoiding browser-based security solutions." 

AWS re:Invent

Recap

AMAZON LAUNCHES PREVIEW OF NEW AWS PRIVATE 5G MANAGED SERVICE

- Amazon revealed the preview of "AWS Private 5G" at its AWS re:Invent conference, which is a new service that seeks to make it easy to establish and operate your own private network.
- AWS Private 5G, according to Amazon, streamlines implementation by allowing users to easily construct their own 4G/LTE or 5G networks, scale up and down the number of connected devices, and take advantage of a familiar on-demand cloud pricing model. [↗](#)

AWS INTRODUCES IOT TWINMAKER, A NEW SERVICE TO EASILY CREATE DIGITAL TWINS

- AWS IoT TwinMaker, a new tool that makes it easy to create and use digital twins of real-world systems, was launched this morning at the company's re:Invent conference.
- For context, digital twins are virtual representations of things like buildings, factories, production lines, and equipment that are updated with real-world data on a regular basis to replicate the behaviour of the systems they represent. [↗](#)

AWS RE:INVENT MAJOR ANNOUNCEMENTS

- Because of Amazon's dominance in the public cloud IaaS and PaaS market, its enormous ecosystem, and its proclivity to introduce hundreds of products and emphasise its innovation roadmap, AWS re:Invent is undoubtedly the industry's most important cloud conference.
- AWS continues to push the price-performance envelope on Graviton2. Newly added capabilities for the Amazon Inspector service will meet the "critical need to detect and remediate at speed" in order to secure cloud workloads... [↗](#)

AWS re:Invent

CELEBRATING 10 YEARS OF RE:INVENT



ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

MOVING TARGET DEFENCE



Due to the static nature of modern day computing systems, they are quite defenseless against the hackers. Hackers make use of the time to tap into the vulnerabilities or gaps in the system and initiate an attack. This is unacceptable as it provides a skewed advantage to the hackers.

This is where Moving Target Defense (MTD) comes into play. It has revolutionized the way defense technology works. Due to the dynamic nature of change that occurs across multiple systems, there is a certain level of uncertainty which hampers the progress of the attackers. It narrows down the window of opportunity for the cyber criminals which leads them to try harder and invest more time and resources but in vain. It further defuncts their surveillance on the system.

Infopercept is in partnership with a leading MTD solutions provider. Together we have strategized a transformational approach to cybersecurity. It is a powerful tool to prevent cyber crimes such as ransomware attacks, fileless attacks, and other web-born exploits. [↗](#)