INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -01 November 2021

Contents

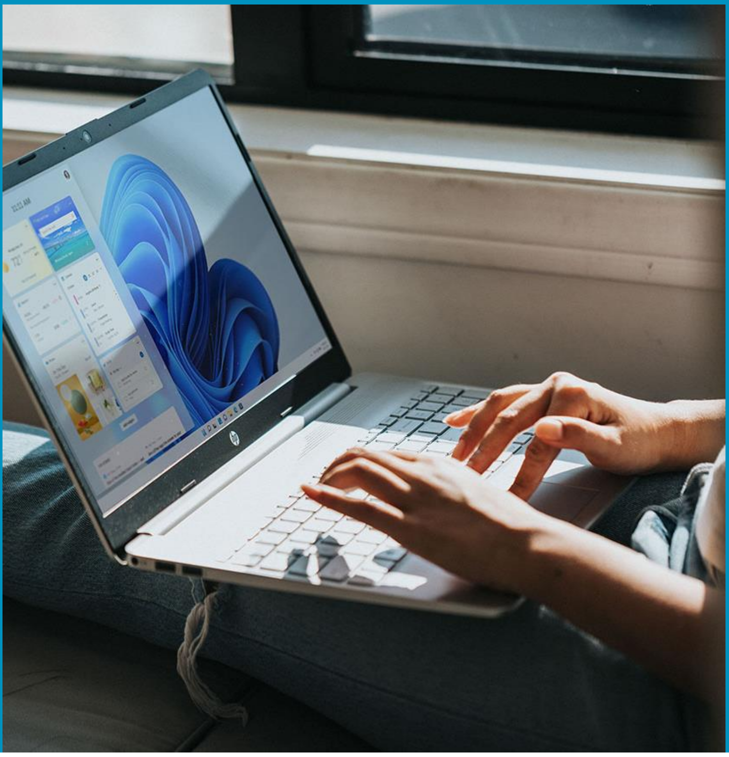
Patch Notes

APPLE PATCHES BUGS IN IOS AND IPADOS

- On two consecutive days Apple has released a few important patches. iOS 14.8.1 comes just a month after releasing iOS 14.8 for those who didn't want to update their iPhones to iOS 15.
- Apple advises users to update to iOS 15.1 and iPadOS 15.1 or iOS 14.8.1 and iPadOS 14.8.1 which can be done through the automatic update function or iTunes.

ADOBE DUMPS MASSIVE SECURITY PATCH UPDATE

- Adobe has issued a vast security update targeting 14 products, including Lightroom, Photoshop, and InDesign. Adobe issued over 80 patches for vulnerabilities, including critical code execution flaws, privilege escalation, denial-of-service, and memory leaks.
- Adobe After Effects, Audition, Bridge, Character Animator, Prelude, Lightroom Classic, Illustrator, Media Encoder, Premiere Pro, Animate, Premiere Elements, InDesign, XMP Toolkit SDK, and Photoshop have all received new updates.



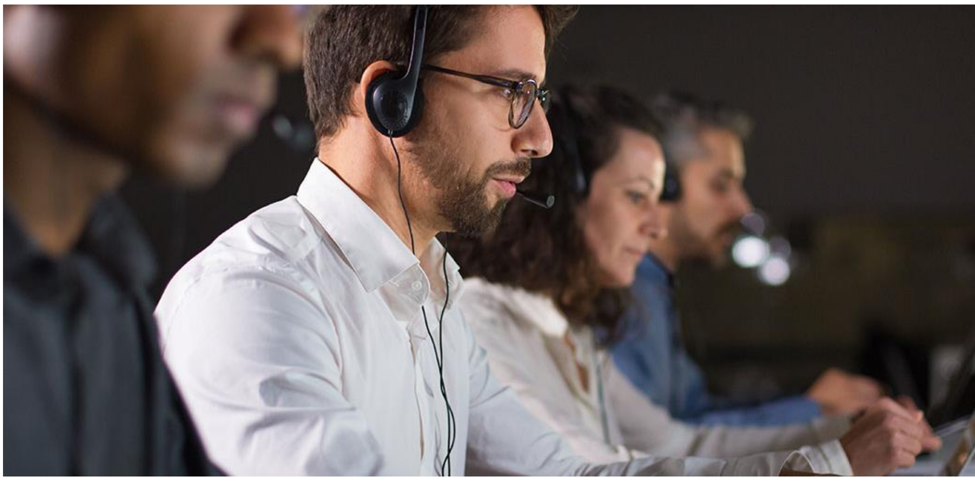
WINDOWS 10 KB5006738 RELEASED WITH FIXES FOR PRINTING ISSUES

- Microsoft has released the optional KB5006738 Preview cumulative update for Windows 10 2004, Windows 10 20H2, and Windows 10 21H1.
- Microsoft says this update and a separate Windows Server preview update will fix all outstanding printing issues affecting users since they mitigated the PrintNightmare vulnerabilities.

CYBER ATTACKS

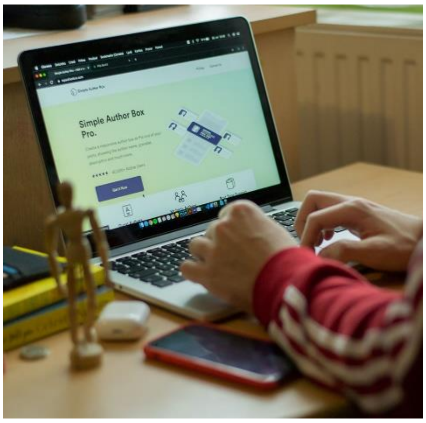
UK council members targeted by distributed denial of service (DDoS) attacks in recent weeks.

- According to an industry association, many UK-based providers of voice over internet protocol (VoIP) services have been hit by a "unprecedented" and coordinated cyber-attack.
- The DDoS attacks on British VoIP companies took place over the last four weeks and "appears to be part of a coordinated extortion-focused international effort by professional cyber-criminals," according to the report.



WORDPRESS PLUGIN VULNERABILITY OPENED UP ONE MILLION SITES TO REMOTE TAKEOVER

- Vulnerabilities in OptinMonster, an email marketing plugin for WordPress, left more than a million websites open to exploitation, security researchers at Wordfence warn.
- Left unaddressed, the flaws make it possible for an unauthenticated attacker to export sensitive information and add malicious JavaScript to vulnerable WordPress sites, among other exploits. The Wordfence Threat Intelligence team notified developers of the plugin about the problem on September 28.



SCUF GAMING STORE HACKED TO STEAL CREDIT CARD INFO OF 32,000 CUSTOMERS

- SCUF Gaming International, a leading manufacturer of custom PC and console controllers, is notifying customers that its website was hacked in February to plant a malicious script used to steal their credit card information.
- Threat actors inject JavaScript-based scripts known as credit card skimmers (aka Magecart scripts, payment card skimmers, or web skimmers)

DATA BREACH AT COLORADO UNIVERSITY IMPACTS 30,000 STUDENTS

- A data breach at a Colorado university has potentially exposed the personal details of 30,000 current and former students.
- The University of Colorado Boulder announced that the incident was a result of a cyber-attack on third-party service Atlassian.Atlassian is a software program used by the institution's Office of Information Technology...

Malware and Vulnerabilities

MALICIOUS NPM LIBRARIES INSTALL RANSOMWARE, PASSWORD STEALER

- The two NPM packages, noblox.js-proxy and noblox.js-proxies, exploit typosquatting to impersonate the official Roblox API wrapper noblox. By changing a single letter in the library's name, it becomes js-proxied.

- The malicious NPM modules will run a postinstall.js script after being added to a project and activated. This script is often used to run lawful actions once a library is installed, but in this case.

BRUTAL WORDPRESS PLUGIN BUG ALLOWS SUBSCRIBERS TO WIPE SITES

- Authenticated attackers can reset and delete affected websites thanks to a high-severity security hole discovered in a WordPress plugin with over 8,000 current instals.

- Authenticated attackers might use the security flaw to reset WordPress sites and erase practically all database content and uploaded media.

UNIQUE AND UNDOCUMENTED MALICIOUS LOADER THAT RUNS AS A SERVER

- ESET researchers have found a hitherto unknown loader for Windows binaries that runs as a server and executes received modules in memory, unlike conventional loaders. We've given this new virus the moniker Wslink, which is the name of one of its DLLs.

- The modules don't have to create new outbound connections because they reuse the loader's routines for communication, keys, and sockets. Wslink also includes a well-developed...

SQUIRRELWAFFLE LEVERAGES MALSPAM TO DELIVER QAKBOT, COBALT STRIKE

- A new threat known as "SQUIRRELWAFFLE" has recently been spreading through spam campaigns, infecting PCs with a new malware loader. This is a virus family that has been spreading with increasing frequency and has the potential to become the next big spam player.

- Threat actors can utilise SQUIRRELWAFFLE to gain an initial foothold on systems and their network environments, which can then be exploited to facilitate further compromise or malware infections,

CYBER TECH

MICROSOFT NOW ROLLING OUT WINDOWS 11 TO MORE ELIGIBLE DEVICES

- Microsoft is now rolling out the Windows 11 upgrade to more eligible Windows devices as part of a phased rollout designed to deliver a smooth upgrade experience.
- According to previously available information, the company estimates that all eligible Windows 10 devices will be offered the upgrade to the latest version by mid-2022. Windows 10 users can upgrade to Windows 11 via Windows Update as long as their computers come with compatible hardware. ↗

MICROSOFT DEFENDER ATP ADDS LIVE RESPONSE FOR LINUX AND MACOS

- Microsoft has announced the addition of new live macOS and Linux response capabilities to Defender for Endpoint, the enterprise version of Redmond's Windows 10 Defender antivirus.
- The new capabilities are now available in public preview in the enterprise endpoint security platform (previously known as ↗

HARDWARE-GRADE ENTERPRISE AUTHENTICATION WITHOUT HARDWARE: NEW SIM SECURITY SOLUTION FOR IAM

- Hardware-based security tokens or dongles have gained popularity, particularly at the enterprise level. They generate a code for the user to enter when prompted, so that only the user possessing the token can gain access.
- One of the ways to use is to implement a passwordless one-tap registration and login solution to access an enterprise system using a companion app. ↗

Infopercept

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.

ENDPOINT DETECTION AND RESPONSE

Endpoint Detection and Response is a type of cyber technology that continually monitors, responds to, and mitigates threats.

The incidents that occur at the endpoints in the network are logged into a central database system where it is further analyzed and investigated by a software agent. An in-depth study into this helps prepare the foundation to be able to anticipate, monitor, and report events for better preparedness for future cyber-attacks.

With the use of analytic tools, ongoing monitoring and detection are facilitated. The tools can help you identify tasks that can improve your organization's overall state of security by identifying, responding to, and deflecting internal threats and external attacks.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN
+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense