

Contents

01 Patches Notes

- Adobe Patches Reader Flaws That Earned Hackers \$150,000 at Chinese Contest
- Cisco Patches Critical Vulnerability in Contact Center Products
- Firefox fixes fullscreen notification bypass bug that could have led to convincing phishing campaigns

02 Cyber Attack

- Mobile Phishing & Managing User Fallibility
- Defense contractor Hensoldt confirms Lorenz ransomware attack
- Phishers are targeting Office 365 users by exploiting Adobe Cloud

03 Malware and Vulnerabilities

- Critical SonicWall NAC Vulnerability Stems from Apache Mods
- Threat actors can bypass malware detection due to Microsoft Defender weakness
- Three Plugins with Same Bug Put 84K WordPress Sites at Risk

04 Cyber-Tech

- A New Approach to Detect Stealthy Malware on IoT Devices
- NoReboot - Faking iPhone Shutdown and Reboot
- Introducing vAPI - an open source lab environment to learn about API security

Patches Notes

CISCO PATCHES CRITICAL VULNERABILITY IN CONTACT CENTER PRODUCTS

- Cisco released security updates for a crucial vulnerability in the Unified Contact Center Management Portal and Domain Manager that could be manipulated remotely to uplift privileges to administrator.
- The issue, tracked as CVE-2022-20658 (CVSS score of 9.6), exists because there was no server-side validation of user permissions, allowing an attacker to send a crafted HTTP request to exploit the flaw on a vulnerable system. [↗](#)



ADOBE PATCHES READER FLAWS THAT EARNED HACKERS \$150,000 AT CHINESE CONTEST

- Adobe announced security updates for several products, including Acrobat and Reader, on Tuesday, patching a total of 26 vulnerabilities.
- The majority of the 26 security holes fixed in the Windows and macOS versions of Acrobat and Reader are memory-related issues that can be exploited for arbitrary code execution. [↗](#)

FIREFOX FIXES FULLSCREEN NOTIFICATION BYPASS BUG THAT COULD HAVE LED TO CONVINCING PHISHING CAMPAIGNS

- The vulnerability (CVE-2022-22746), which existed in Windows versions of Firefox, is a race condition bug that could cause the browser's fullscreen notification warning to be ignored.
- Controlling a fullscreen browser window without the user's knowledge allows the attacker to spoof the URL address bar of a legitimate site - something that is normally controlled by the browser, along with other 'above the line' trust indicators. [↗](#)

MOBILE PHISHING & MANAGING USER FALLIBILITY

- Increasingly, mobile phishing is the culprit. The annualized risk of a data breach resulting from phishing attacks has a value of about \$1.7 million.
- As part of a zero-trust strategy, organizations should look to the following strategies:.
Leverage machine learning to conduct continuous device posture assessment, role-based user access control and location awareness before granting access to data. [↗](#)

CYBER ATTACKS



DEFENSE CONTRACTOR HENSOLDT CONFIRMS LORENZ RANSOMWARE ATTACK

- Hensoldt, a multinational defence contractor headquartered in Germany, has confirmed that a ransomware attack compromised some of its UK subsidiary's systems.
- Since December 17, 2021, when the Hensoldt leak page was first created, the gang has published 95 percent of all stolen files published on the ransomware's data leak website as password-protected archives. [↗](#)




PHISHERS ARE TARGETING OFFICE 365 USERS BY EXPLOITING ADOBE CLOUD

- Phishers are creating Adobe Creative Cloud accounts and using them to send phishing emails that can evade traditional security measures as well as some advanced threat protection solutions.
- This new wave of attacks began in December 2021, and it takes advantage of the fact that Adobe's apps are designed to foster collaboration through document sharing. [↗](#)



Malware and Vulnerability



CRITICAL SONICWALL NAC VULNERABILITY STEMS FROM APACHE MODS

- Rapid7 has released additional information about a SonicWall critical flaw that allows for unauthenticated remote code execution on affected devices
- The flaw (CVE-2021-20038) is one of five discovered in its popular network access control (NAC) system products [↗](#)



THREAT ACTORS CAN BYPASS MALWARE DETECTION DUE TO MICROSOFT DEFENDER WEAKNESS

- As a result of a flaw in Microsoft Defender antivirus, attackers may be able to retrieve information that they can use to avoid detection.
- Threat actors can exploit a flaw in Microsoft Defender antivirus to determine which folders to plant malware in in order to avoid AV scanning. [↗](#)

THREE PLUGINS WITH SAME BUG PUT 84K WORDPRESS SITES AT RISK

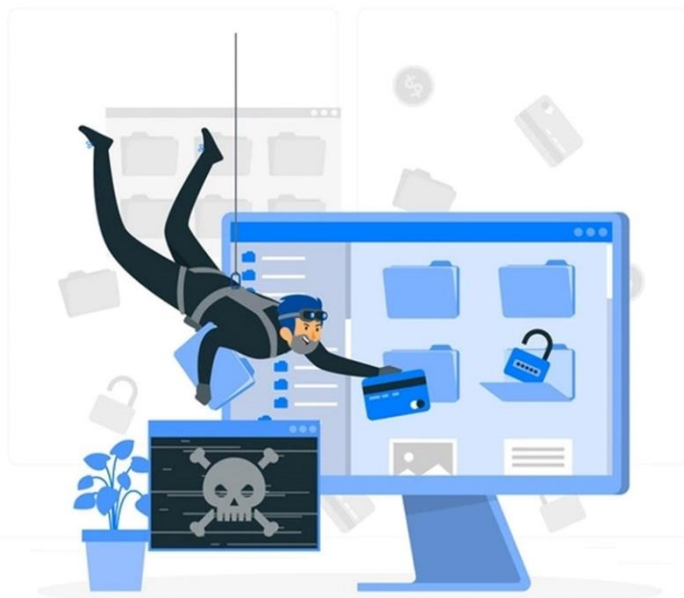
- Researchers discovered three plug-ins with the same vulnerability that allows an attacker to update arbitrary site options on a vulnerable site and completely take it over.
- Recommended actions for WordPress users are to verify that their site has been updated to the latest patched version available for each of them. Exploiting Arbitrary Options. [↗](#)

CYBER TECH



A NEW APPROACH TO DETECT STEALTHY MALWARE ON IOT DEVICES

- Security teams have developed a new approach that uses electromagnetic field emanations to detect evasive malware on IoT devices.
- Side channel details are used by hackers to detect anomalies in emanations that differ from previously observed patterns and suspicious behaviour in the system's normal state. [↗](#)



NOREBOOT - FAKING IPHONE SHUTDOWN AND REBOOT

- A proof-of-concept demonstrated that simulates an iPhone reboot or shutdown in order to prevent malware removal.
- The proof-of-concept includes specially crafted code injected into three iOS daemons that simulate the shutdown process by disabling all key indicators. [↗](#)

INTRODUCING VAPI - AN OPEN SOURCE LAB ENVIRONMENT TO LEARN ABOUT API SECURITY

- API security has become a key topic of concern. APIs are increasingly widely utilised to handle services and data transfers, and a single faulty endpoint can result in data breaches or network intrusions in a business.
- vAPI could be useful to new penetration testers in acclimating them to how different API bugs are classified, as well as developers, because the platform allows them to see examples of vulnerable code - and consider potential mitigations [↗](#)



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. 



SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117

sos@infopercept.com

www.infopercept.com

