

Contents

01 Patches Notes

02 Cyber Attack

03 Malware and Vulnerabilities

04 Cyber-Tech

“

**THERE'S NO SILVER BULLET
SOLUTION WITH CYBER
SECURITY, A LAYERED
DEFENSE IS THE ONLY
VIABLE DEFENSE.**



Patches Notes

FORTINET SECURITY FOR HACKERS UNAUTHENTICATED ACCESS

- Fortinet has issued updates to its FortiManager and FortiAnalyzer network management tools to address a critical vulnerability that may be exploited to execute arbitrary code with elevated privileges.
- Fortinet has issued a security warning for the problem, which is presently tracked as CVE-2021-32589, stating that it is a use-after-free (UAF) vulnerability in the fgmsd daemon in FortiManager and FortiAnalyzer. [↗](#)

ADOBE PATCHES 21 VULNERABILITIES ACROSS SEVEN PRODUCTS

- Adobe published security patches for seven of its products on Tuesday, patching a total of 21 vulnerabilities, including 15 issues with severe severity ratings.
- Adobe After Effects for Windows and macOS has been patched to address seven vulnerabilities. Five of these can allow arbitrary code execution and have been classified critical, however it's worth noting that based on their CVSS score, they are truly high-severity problems. [↗](#)

CHROME BROWSER PATCH ZERO-DAY BUG EXPLOITED IN THE WILD

- Google has released a new security update for the Chrome browser for Windows, Mac, and Linux that includes numerous patches, including a zero-day vulnerability that it claims is being exploited in the wild.
- The new patch fixes eight vulnerabilities, one of which is a type confusion problem in its V8 open-source and JavaScript engine (CVE-2021-30563). [↗](#)



FORTINET®

SAUDI ARAMCO DATA BREACH SEES 1 TB STOLEN DATA FOR SALE

- The Saudi Arabian Oil Company, or Saudi Aramco, obtained 1 TB of private data and is selling it on the darknet.
- The oil company employs about 66,000 people and generates almost \$230 billion in revenue each year. Threat actors are selling Saudi Aramco's data for a negotiated fee of \$5 million. [↗](#)

CYBER ATTACKS



UPDATED JOKER MALWARE FLOODS INTO ANDROID APPS

- The Joker mobile virus is back on Google Play, and there has been an increase in dangerous Android apps that disguise the billing-fraud software.
- Since September, at least 1,000 additional samples have been identified in the newest wave, with many of them making their way into the legitimate market.



PEGASUS SPYWARE USED TO TARGET PHONES OF JOURNALISTS

- A 17-media investigation discovered that NSO Group's Pegasus software was used in hacking attempts on 37 cell phones belonging to human rights activists and journalists.
- According to "The Guardian," Pegasus can retrieve all of a mobile device's data and activate the device's microphone to listen in on conversations secretly. [↗](#)

Malware and Vulnerabilities



NEW WINDOWS DEFENDER MALWARE EXCLUSIONS TO EVADE DETECTION HIDES ITSELF AMONG

- On Tuesday, cybersecurity experts revealed the existence of a previously unknown malware strain known as "MosaicLoader," which targets people looking for cracked software as part of a global campaign.
- MosaicLoader's creators-built malware that can deliver any payload on the system, making it potentially profitable as a delivery service. [↗](#)



RESEARCHER UNCOVERS YET ANOTHER UNPATCHED WINDOWS PRINTER SPOOLER

- Only days after Microsoft issued a warning about an unpatched security hole in the Windows Print Spooler service, another potentially zero-day problem in the same component has been identified, making it the fourth printer-related flaw reported in recent weeks.
- A security researcher disclosed an attack for the issue. By connecting to a rogue print server... [↗](#)

SONICWALL WARNS USERS OF "IMMINENT RANSOMWARE CAMPAIGN"

- SonicWall has issued a "urgent security notification" to customers, warning them of ransomware attacks targeting unpatched end-of-life (EoL) Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) products.
- "Organizations who do not take necessary steps to address these vulnerabilities on their SRA and SMA 100 series devices are at danger of a targeted ransomware attack," SonicWall cautions. [↗](#)

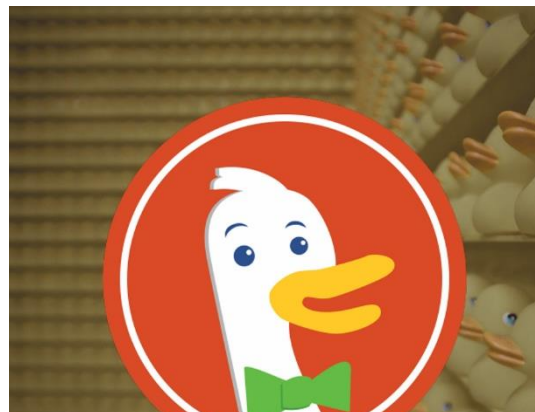
HIVENIGHTMARE ZERO-DAY LETS ANYONE BE SYSTEM ON WINDOWS 10 AND 11

- On Windows 10 and Windows 11, users with low rights can access critical Registry database files, making them vulnerable to SeriousSAM or HiveNightmare, a local elevation of privilege vulnerability.
- A user can utilise SeriousSAM to access a variety of system files, including the Security Accounts Manager (SAM) database. [↗](#)

CYBER TECH

MITRE ANNOUNCES FIRST EVALUATIONS OF CYBERSECURITY TOOLS FOR INDUSTRIAL CONTROL SYSTEMS

- MITRE Engenuity released the findings of its first-ever ATT&CK Evaluations for Industrial Control Systems on Monday (ICS).
- MITRE researchers utilised the Triton virus to evaluate the detection capabilities of five different cybersecurity products from ICS manufacturers. Many of the world's most important infrastructures, such as energy transmission and distribution plants, oil refineries, wastewater treatment facilities, and others, rely on industrial control systems. [↗](#)



DUCKDUCKGO'S NEW EMAIL PRIVACY SERVICE FORWARDS TRACKER-FREE MESSAGES

- DuckDuckGo is putting out an email privacy feature that removes trackers from incoming messages, allowing for improved profiling and ad targeting.
- Users of the service are given a free "@duck.com" email account, which cleans messages of trackers and sends them to their regular inbox. Trackers can notify email senders when you read their messages and assist advertising businesses in creating a profile for you based on acquired metadata. [↗](#)

MICROSOFT DEFENDER FOR IDENTITY NOW DETECTS PRINTNIGHTMARE

- Microsoft has introduced PrintNightmare exploitation detection capability to Microsoft Defender for Identity in order to assist Security Operations teams in detecting attackers' efforts to exploit this severe vulnerability.
- According to Microsoft, Defender for Identity now detects Windows Print Spooler service exploitation (including the currently exploited CVE-2021-34527 PrintNightmare flaw) and aids in the prevention of lateral ... [↗](#)



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.

TECHNOLOGY ADVISORY SERVICES



One of the most critical components of a successful business is technology. But is your current technology in line with your organization's roadmap to success?

The right technology in your organization will help your business make the best use of the information and the resources, whilst empowering you to execute to the best of your abilities at functional and strategic levels. However, successful technology involves much more than just choosing a system. An organization should have the right balance of people, processes, and technology, so that it will help your business to grow.

Infopercept can assist your organization by guiding you through the complexities of technology selection and implementation, by managing and designing business processes and coordinating resources to maximize your return on investment. 



SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117

sos@infopercept.com

www.infopercept.com

