INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -15 November 2021

Contents

01 Patch Notes

- Microsoft urges Exchange admins to patch bug exploited in the wild
- Microsoft November 2021 Patch Tuesday: 55 bugs squashed, two under active exploit
- Apache Storm maintainers patch two pre-auth RCE vulnerabilities

02 Cyber Attack

- DDoS Attacks Shatter Records in Q3, Report Finds
- Robinhood Trading App Suffers Data Breach Exposing 7 million Users' Information
- DDoS Attack on VoIP Provider Telnyx Impacts Global Telephony Services

03 Malware and Vulnerabilities

- Massive Zero-Day Hole Found in Palo Alto Security Appliances
- Zoho Password Manager Flaw Torched by Godzilla Webshell
- BrakTooth Bluetooth Bugs Bite: Exploit Code, PoC Released

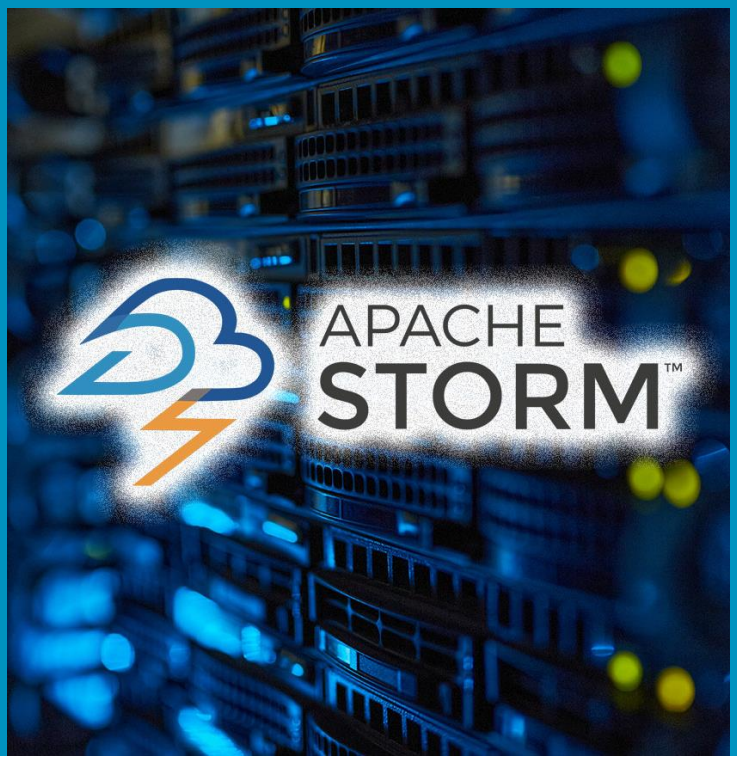
04 Cyber-Tech

- Microsoft: Windows 10 2004 reaches end of service next month
- OneDrive reaches end of support on Windows 7, 8 in January
- Windows 11 KB5007215 update released with application fixes

Patch Notes

MICROSOFT URGES EXCHANGE ADMINS TO PATCH BUG EXPLOITED IN THE WILD

- Microsoft warned admins today to immediately patch a high severity Exchange Server vulnerability that may allow authenticated attackers to execute code remotely on vulnerable servers.
- The security flaw tracked as CVE-2021-42321 impacts Exchange Server 2016 and Exchange Server 2019, and it is caused by improper validation of cmdlet arguments according to Redmond's security advisory.



MICROSOFT NOVEMBER 2021 PATCH TUESDAY: 55 BUGS FIXED, TWO UNDER ACTIVE EXPLOIT

- On what might seem a relatively calm Patch Tuesday with 55 vulnerabilities being patched, the fact that six of them were rated “Critical” and two of them actively exploited spoils the Zen factor somewhat.
- Exploits fixed are related to the following components: Exchange Server, Excel, RDP, Windows Defender, 3D Viewer, etc.

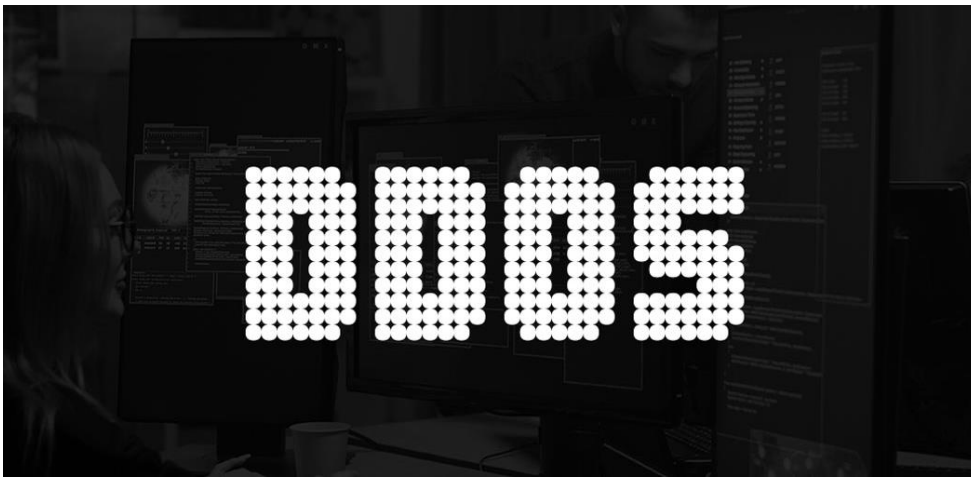
APACHE STORM MAINTAINERS PATCH TWO PRE-AUTH RCE VULNERABILITIES

- Apache Storm, an open source real-time streaming data analytics platform, has patched two vulnerabilities that led to remote code execution (RCE).
- Discovered and reported by GitHub Security Lab, the bugs included a command injection vulnerability and an unsafe deserialization bug.

CYBER ATTACKS

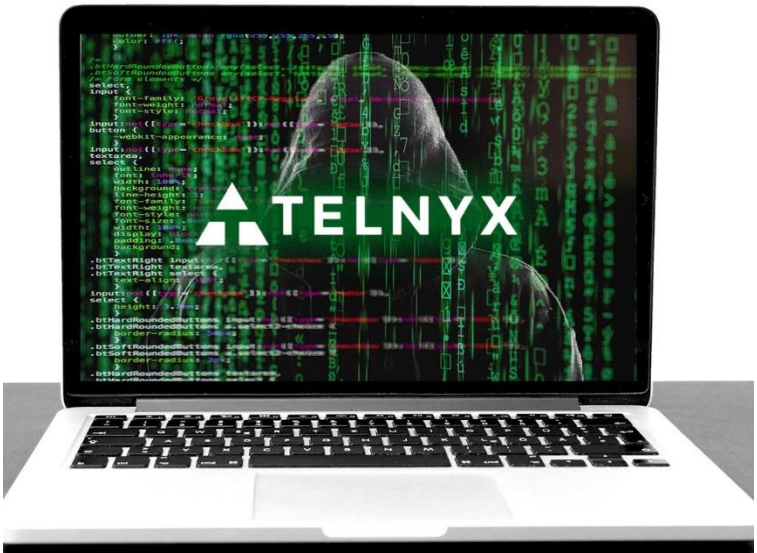
DDoS Attacks Shatter Records in Q3 of 2021

- The latest DDoS report for Q3 from Kaspersky details a record-breaking frenzy of recent activity by threat actors.
- The third quarter saw the sheer volume of distributed denial-of-service (DDoS) attacks surge to several thousand hits per day, signalling a re-distribution of tactics by malicious actors away from crypto mining and toward the use of DDoS as a tool of intimidation, disinformation and straight-up extortion.



ROBINHOOD TRADING APP SUFFERS DATA BREACH EXPOSING 7 MILLION USERS' INFORMATION

- Robinhood on Monday disclosed a security breach affecting approximately 7 million customers, roughly a third of its user base, that resulted in unauthorized access of personal information by an unidentified threat actor.
- The commission-free stock trading and investing platform said the incident happened "late in the evening of November 3," adding it's in the process of notifying affected users.



DDOS ATTACK ON VOIP PROVIDER TELNYX IMPACTS GLOBAL TELEPHONY SERVICES

- Attackers can disrupt global telephony services too, and the DDoS attack on Telnyx is a recent example.
- Telnyx confirmed that it sustained the increasing intensity of DDoS attacks twice in a day.DDoS attacks could create huge damage to victims' operations, making it difficult for a single defender to stop the flood of incoming traffic.

Malware and Vulnerabilities

MASSIVE ZERO-DAY HOLE FOUND IN PALO ALTO SECURITY APPLIANCES

- Researchers have developed a working exploit to gain remote code execution (RCE) via a massive vulnerability in a security appliance from Palo Alto Networks (PAN), potentially leaving 10,000 vulnerable firewalls with their goods exposed to the internet.
- The critical zero day, tracked as CVE 2021-3064 and scoring a CVSS rating of 9.8 out of 10 for vulnerability severity, is in PAN's GlobalProtect firewall.

ZOHO PASSWORD MANAGER FLAW TORCHED BY GODZILLA WEBSHELL

- A new campaign is prying apart a known security vulnerability in the Zoho ManageEngine ADSelfService Plus password manager, researchers warned over the weekend.
- The threat actors have managed to exploit the Zoho weakness in at least nine global entities across critical sectors so far (technology, defence, healthcare, energy and education), deploying the Godzilla web shell and exfiltrating data.

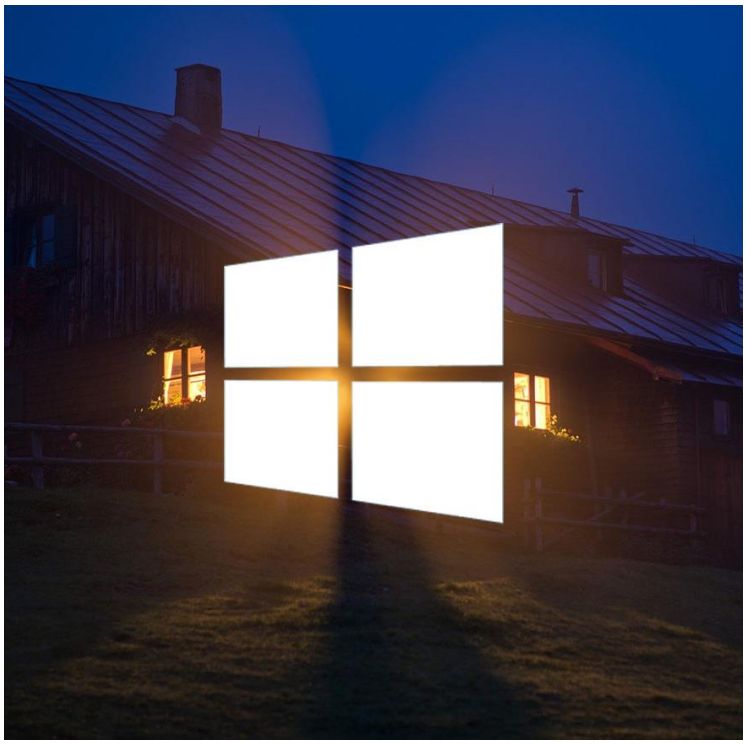
BRAKTOOTH BLUETOOTH BUGS EXPLOIT CODE and POC RELEASED

- The embargo period is over for a proof-of-concept (PoC) tool to test for the recently revealed BrakTooth flaws in Bluetooth devices, and the researchers who discovered them have released both the test kit and full exploit code for the bugs.
- On Thursday, CISA urged manufacturers, vendors and developers to patch or employ workarounds.Researchers from the University of Singapore disclosed the initial group of 16 vulnerabilities (now up to 22), collectively dubbed BrakTooth, in a paper published in September.

CYBER TECH

MICROSOFT: WINDOWS 10 2004 REACHES END OF SERVICE NEXT MONTH

- Microsoft has reminded users today that all editions of Windows 10, version 2004 and Windows Server, version 2004 (also known as the Windows 10 May 2020 Update), will reach end of servicing on December 14, 2021.
- Customers still using end of service software are advised to upgrade to the latest version of Windows 10 (21H1 aka the May 2021 Update) or to Windows 11 (if they have eligible devices) as soon as possible to keep their systems secure and bug-free.



ONEDRIVE REACHES END OF SUPPORT ON WINDOWS 7, 8 IN JANUARY

- Microsoft has announced that the OneDrive desktop application will reach the end of support on legacy Windows 7, 8, and 8.1 starting with January 1, 2022.
- Customers with systems still running Windows 7, 8, or 8.1 are advised to upgrade their OS to Windows 10 or Windows 11. On devices that don't meet the upgrade requirements, users can still back up their files to the cloud by manually uploading them to OneDrive on the web.

WINDOWS 11 KB5007215 UPDATE RELEASED WITH APPLICATION

- Microsoft has released the Windows 11 KB5007215 cumulative update to fix security vulnerabilities and bugs introduced in previous versions.
- Last week, Microsoft added a new known issue for apps using GDI+ that prevented drawing or the proper display of user interface elements. With this update, Microsoft has fixed this issue, and GDI+ applications should be working again.

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.

IDENTITY ACCESS MANAGEMENT

Identity Access Management is a combination of business policies and technologies that facilitates the management of electronic digital identities. With an IAM framework in place, IT managers can control and moderate a particular user's access to critical information within an organization.

Identity and Access Management allows system administrators to utilize role based access control. This lets the administrators assign a particular role to an individual that defines his information access scope and capabilities within an enterprise's information system or networks.

Infopercept specializes in combining all of the necessary control and tools to capture and record user login information, manage the enterprise database of user identities and orchestrate the assignment and removal of access privileges. Ensuring that the implemented IDAM solution provides a centralized directory service with monitoring as well as visibility over every aspect of an organization's user base.

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

INVINSENSE™
Attacktical Cybersecurity Sense