INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -13 Sep 2021

Contents

Patches Notes

CRITICAL AUTH BYPASS BUG AFFECT NETGEAR SMART SWITCHES — PATCH AND POC RELEASED

- Networking, storage and security solutions provider Netgear on Friday issued patches to address three security vulnerabilities affecting its smart switches that could be abused by an adversary to gain full control of a vulnerable device.

- The critical nature of the vulnerabilities, companies relying on the aforementioned Netgear switches are recommended to upgrade to the latest version as soon as possible to mitigate any potential exploitation risk.

WHATSAPP PATCHES VULNERABILITY RELATED TO IMAGE FILTER FUNCTIONALITY

- Check Point Research has announced the discovery of a vulnerability in the popular messaging platform WhatsApp that allowed attackers to read sensitive information from WhatsApp's memory.

- The messaging platform -- considered the most popular globally with about two billion monthly active users -- had an "Out-Of-Bounds read-write vulnerability" related to the platform's image filter functionality, according to Check Point Research.

ZOHO PATCHES ACTIVELY EXPLOITED CRITICAL ADSELFSERVICE PLUS BUG

- Hackers are exploiting a critical vulnerability in Zoho’s ManageEngine ADSelfService Plus password management solution that allows them to take control of the system.

- ADSelfService Plus is aimed at larger organizations that need an integrated self-service password management for and single sign-on solution for Active Directory and cloud apps.

GOOGLE ANDROID SECURITY UPDATE PATCHES 40 VULNERABILITIES

- Google on 07th September 2021, published the Android Security Bulletin for September 2021 with patches for a total of 40 vulnerabilities, including seven that are rated critical.

- A total of 16 issues were patched with the first part of this month’s security updates – the 2021-09-01 security patch level – including one critical issue in the Framework component. Tracked as CVE-2021-0687, the security bug affects Android 8.1, 9, 10, and 11.

CYBER ATTACKS

RANSOMWARE ATTACKS INCREASED BY 288% IN H1 2021

- The growing threat of ransomware around the world. Number of ransomware attacks analysed by the team has increased by 288% between January-March 2021 and April-June 2021
- The victims of this ransomware strain have faced data encryption, the threat of data leaks, and the wider risk of DDoS attacks disrupting operations, the strain is now believed to be inactive.

HACKERS LEAK VPN ACCOUNT PASSWORDS FROM 87,000 FORTINET FORTIGATE DEVICES

Network security solutions provider Fortinet confirmed that a malicious actor had unauthorizedly disclosed VPN login names and passwords associated with 87,000 FortiGate SSL-VPN devices.

An threat actor leaked a list of Fortinet credentials for free on a new Russian-speaking forum called RAMP that launched in July 2021 as well as on Groove ransomware's data leak site, with Advanced Intel noting that the "breach list contains raw access to the top companies" spanning across 74 countries, including India, Taiwan, Italy, France, and Israel. "2,959 out of 22,500 victims are U.S. entities,"

MCDONALD'S LEAKS PASSWORD FOR MONOPOLY VIP DATABASE TO WINNERS

- A bug in the McDonald's Monopoly VIP game in the United Kingdom caused the login names and passwords for the game's database to be sent to all winners.
- The error clearly stated that both a production and staging server's credentials were leaked, McDonald's confirms that it was only the staging server that was exposed.

Malware and Vulnerabilities

GITHUB FINDS 7 CODE EXECUTION VULNERABILITIES IN 'TAR' AND NPM CLI

- GitHub security team has identified several high-severity vulnerabilities in npm packages, "tar" and "@npmcli/arborist," used by npm CLI.

- Node.js package tar remains a core dependency for installers that need to unpack npm packages post-installation. The package is also used by thousands of other open source projects, and as such receives roughly 20 million downloads every week.

LATEST ATLASSIAN CONFLUENCE FLAW EXPLOITED TO BREACH JENKINS PROJECT SERVER

- The Jenkins project says it has fallen prey to widespread attacks targeting a critical vulnerability in Confluence, Atlassian's team collaboration software.

- Attackers compromised Jenkins' deprecated Confluence service last week, revealed the team behind the eponymous open source automation server on Saturday (September 4).

NEW 0-DAY ATTACK TARGETING WINDOWS USERS WITH MICROSOFT OFFICE DOCUMENTS

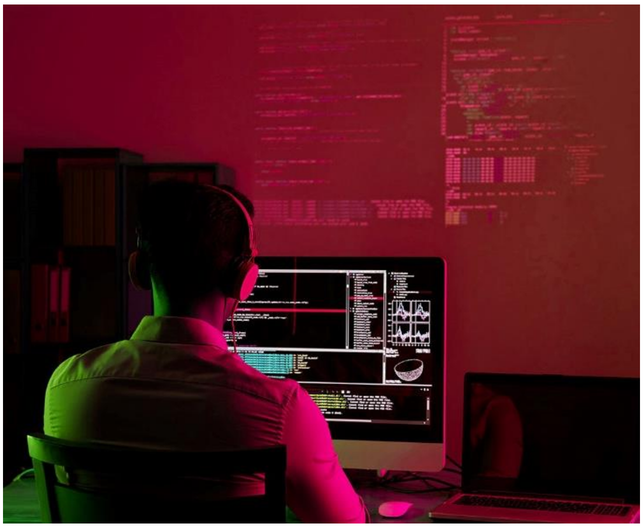
- Microsoft on Tuesday warned of an actively exploited zero-day flaw impacting Internet Explorer that's being used to hijack vulnerable Windows systems by leveraging weaponized Office documents.

- Tracked as CVE-2021-40444 (CVSS score: 8.8), the remote code execution flaw is rooted in MSHTML (aka Trident), a proprietary browser engine for the now-discontinued Internet Explorer and which is used in Office to render web content inside Word, Excel, and PowerPoint documents.

CYBER TECH

TEAMTNT'S NEW TOOLS TARGET MULTIPLE OS

- (The attackers are indiscriminately striking thousands of victims worldwide with their new "Chimaera" campaign.
- The TeamTNT malware pushers have a slew of new toys with which to wreak havoc – multiple shell/batch scripts, open-source tools, a cryptocurrency miner, an IRC and more – that have inflicted more than 5,000 infections globally as antivirus (AV) tools struggle to catch up with the newest malware.



NCCOE RELEASES CYBERSECURITY GUIDE FOR FIRST RESPONDERS

- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has released the final version of a Cybersecurity Practice Guide for first responders.
- The new Cybersecurity Practice Guide was created with the aim of resolving authentication issues so that sensitive data can be accessed by PSFRs both securely and quickly enough to prevent any delay in the provision of potentially life-saving care.

NEW CHAINSAW TOOL HELPS IR TEAMS ANALYZE WINDOWS EVENT LOGS

- Incident responders and blue teams have a new tool called Chainsaw that speeds up searching through Windows event log records to identify threats.
- The tool is designed to assist in the first-response stage of a security engagement and can also help blue teams triage entries relevant for the investigation.

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