INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -29 November 2021

Contents

Patches Notes

NETGEAR FIXES CODE EXECUTION FLAW IN MANY SOHO DEVICES

- Netgear has released a fix for a vulnerability on several of their product models. The affected product models include extenders, routers, air cards, and modems.
- This vulnerability is listed under CVE-2021-34991 and described as a vulnerability that allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6400v2 1.0.4.106_10.0.80 routers. Authentication is not required to exploit this vulnerability.

VMWARE ADDRESSES SSRF, ARBITRARY FILE READ FLAWS IN VCENTER SERVER

- VMware has released security updates for vCenter Server after fixing arbitrary file read and server-side request forgery (SSRF) vulnerabilities in the vSphere Web Client (FLEX/Flash).
- With a CVSS rating of 7.5, the most severe is the arbitrary file read bug (CVE-2021-21980), abuse of which could potentially enable a malicious actor to gain access to sensitive information.

EXPLOIT RELEASED FOR MICROSOFT EXCHANGE RCE BUG, PATCH NOW

- Proof-of-concept exploit code has been released online over the weekend for an actively exploited high severity vulnerability impacting Microsoft Exchange servers.
- The security bug tracked as CVE-2021-42321 impacts on-premises Exchange Server 2016 and Exchange Server 2019 (including those used by customers in Exchange Hybrid mode) and was patched by Microsoft during this month's Patch Tuesday.

CYBER ATTACKS

Millions of GoDaddy customer data compromised in breach

- Domain name registrar giant and hosting provider GoDaddy on 22nd November 2021 disclosed to the Securities and Exchange Commission (SEC) that it had suffered a security breach.
- According to initial investigations, the intruder used a compromised password to access legacy code in GoDaddy's environment to steal data. Investigations are ongoing.

OVER NINE MILLION ANDROID DEVICES INFECTED BY INFO-STEALING TROJAN

- A large-scale malware campaign on Huawei's AppGallery has led to approximately 9,300,000 installs of Android trojans masquerading as over 190 different apps.
- The trojan is detected by Dr.Web as 'Android.Cynos.7.origin' and is a modified version of the Cynos malware designed to collect sensitive user data.

MALWARE NOW TRYING TO EXPLOIT NEW WINDOWS INSTALLER ZERO-DAY

- Malware creators have already started testing a proof-of-concept exploit targeting a new Microsoft Windows Installer zero-day/
- The vulnerability in question is a local privilege elevation bug found as a bypass to a patch Microsoft released during November 2021's Patch Tuesday to address a flaw tracked as CVE-2021-41379.

Malware and Vulnerabilities

CISCO FLAW AFFECTS FIREWALLS

- A newly discovered vulnerability found in two devices made by Cisco could cause remote access to be disrupted.
- If the vulnerability is exploited, the organization's firewall will be weakened, leaving it more vulnerable to attack, and employees who are working remotely would be blocked from accessing their organization's internal network.

NEW WINDOWS ZERO-DAY WITH PUBLIC EXPLOIT LETS YOU BECOME AN ADMIN

- A security researcher has publicly disclosed an exploit for a new Windows zero-day local privilege elevation vulnerability that gives admin privileges in Windows 10, Windows 11, and Windows Server.
- The vulnerability affects all supported versions of Windows, including Windows 10, Windows 11, and Windows Server 2022.

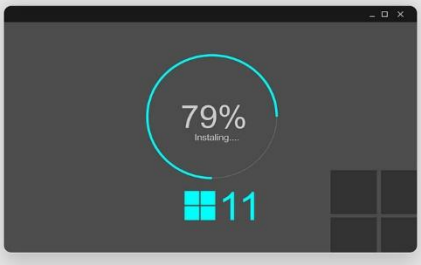
LINUX_AVP: A NEW MALWARE TARGETING E-COMMERCE WEBSITES

- A new Linux backdoor, named linux_avp, has been discovered abusing weaknesses in e-commerce sites around the world. Experts claim it was receiving commands from a control server located in Beijing.
- According to researchers, the attackers are exploiting weaknesses in e-commerce portals to deploy linux_avp, along with a credit card skimmer, to steal payment information from the targeted websites.

NEW VARIANT OF JOKER SPREADING VIA PLAY STORE

- A new set of variants of Joker malware has been discovered spreading via the Play Store. These variants make use of sophisticated techniques to avoid Google's malware detection engine.
- The new variant present in the flasher app is performing malicious activities using three multi-stage payloads. Moreover, this variant request 18 different permissions from Android, out of which the malware uses three permissions.

CYBER TECH



WINDOWS 11 KB5007262 CUMULATIVE UPDATE PREVIEW RELEASED

- Microsoft has released the optional KB5007262 Preview cumulative update for Windows 11 with 70 fixes or improvements.
- This Windows 11 cumulative update is part of Microsoft's November 2021 monthly "C" update, allowing users to test the upcoming updates and fixes in the December 2021 Patch Tuesday.

MICROSOFT UNVEILS 'SUPER DUPER SECURE MODE' IN LATEST VERSION OF EDGE

- Microsoft has unveiled a 'Super Duper Secure Mode' in the latest version of Edge browser, offering users greater protection against common vulnerabilities.
- Super Duper Secure Mode – also known as SDSM – helps to mitigate against browser attacks by disabling the Just-In-Time component in V8, a technology linked a large number of security vulnerabilities in recent years.

A NEW DUCKDUCKGO TOOL IS SUPPOSED TO PREVENT APPS FROM TRACKING ANDROID USERS

- DuckDuckGo's new tool aims to prevent apps from tracking Android users.
- Once App Tracking Protection is enabled, it will run in the background as you use your phone. The tool recognizes when an app is about to send data to a third-party tracker, and will then prevent the app from taking your information.

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.

SECURITY ORCHESTRATION AUTOMATION & RESPONSE

Security Orchestration, Automation, and Response solutions bring out the best in cybersecurity by efficiently combining automation, orchestration & threat data collection from multiple sources and automatically responding to low level security events without human assistance. The goal of using a SAOR stack is to improve the efficiency of physical & digital security operations and to have a single and comprehensive incident response platform.

Infopercept conducts the following steps to implement SOAR;

- Threat and Vulnerability Management
- Security Incident Response
- Incident Report Automation
- Security Operations Automation

For most large-scale environments, having a dedicated 24/7 Digital Security workforce is a must-have, to minimize human errors, handle low tier repetitive tasks and continuous unabated security monitoring. A well-implemented SOAR effectively improves SOC efficiency, provides unprecedented visibility and reduces time-to-respond.

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

INVINSENSE™
Attacktical Cybersecurity Sense