September 20, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Flaws Discovered in Azure App that Microsoft Secretly Installs on Linux VMs
- Malware targets Windows Subsystem for Linux to Evade Detection
- Citrix Patches Hypervisor Vulnerabilities Allowing Host Compromise
- SAP Patches critical vulnerabilities
- Code execution vulnerability in Nitro Pro PDF
- Legacy IBM System X Servers not getting patches for High-Severity Bug

CryptoGen Nepal

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, eBay, eset, BugCrowd, under armour, Coinbase, CCM, etc. have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

Critical Flaws Discovered in Azure App that Microsoft Secretly Installs on Linux VMs

Description	
Microsoft has patched four serious vulnerabilities known as OMIGOD, which were discovered in the Open Management Infrastructure (OMI) software agent, which was quietly deployed on more than half of Azure Linux computers. OMI is a software service for IT management with support for most UNIX systems and modern Linux platforms, used by multiple Azure services, including Open Management Suite (OMS), Azure Insights, Azure Automation. The list of flaws, collectively called OMIGOD, affect a little-known software agent called Open Management Infrastructure that's automatically deployed in many Azure services are Open Management Infrastructure Remote Code Execution Vulnerability, Open Management Infrastructure Elevation of Privilege Vulnerability.	
Source	
Infected Technology	• Azure Automation • Azure Automatic Update • Azure Operation management Suite (OMS) • Azure Log Analytics • Azure Configuration Management • Azure Diagnostics
Recommendation	Update the patch available
CVE_ID	CVE-2021-38647, CVE-2021-38648, CVE-2021-38645, CVE-2021-38649

Malware targets Windows Subsystem for Linux to Evade Detection

Description	
Black Lotus Labs, a threat research group identified vulnerable files in Windows Subsystem for Linux (WSL). These vulnerable ELF files are Python3 code that acted as loader which allows access to remote file and injection to running process. The files can be used to download shellcode from remote command-and-control server and employ PowerShell to carry later movement in the host	
Source	https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders/
Infected Technology	Windows Subsystem for Linux

WordPress 5.8.1 Patches Several Vulnerabilities

Description	
WordPress 5.4-5.8 are affected by multiple Vulnerabilities that an attacker could exploit to take control of an affected website. Three security flaws in the core codebase of WordPress include data exposure vulnerability within the REST API, an interface that allows plugins and themes to interact with WordPress core, Cross-site scripting vulnerability in the Gutenberg block editor, and multiple vulnerabilities in the Lodash JavaScript that are rated critical to high severity.	
Source	https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/
Infected Technology	WordPress
Recommendation	Upgrade to WordPress 5.8.1

Citrix Patches Hypervisor Vulnerabilities Allowing Host Compromise

Description	
Citrix security teams announced the release of multiple security patches that will address critical flaws detected in Hypervisor. The most severe of these vulnerabilities, would allow host compromise due to Grant v2 status pages being unassigned under certain conditions, causing vulnerable software to map them to other locations. A guest virtual machine could maintain access to pages that could have been released and then reused for another purpose, so the malicious code executed on this virtual machine could have 2 or more virtual CPUs assigned.	
Source	https://support.citrix.com/article/CTX325319
Infected Technology	Citrix Hypervisor
Recommendation	Update the latest available Hotfixes for Citrix Hypervisor 7.1
CVE-ID	CVE-2021-28697

SAP Patches critical vulnerabilities

Description	
SAP patches multiple vulnerabilities with September Security Patch. Seven of those vulnerabilities are rated critical. One of the critical vulnerability is missing authorization check in NetWeaver Application server with score of 10 while two 9.9 score vulnerabilities were unrestricted file upload and code injection. Other vulnerabilities include SQL injection, code injection and reflected XSS	
Source	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=585106405
Infected Technology	Multiple SAP products
Recommendation	Apply patches released
CVE-ID	CVE-2021-37535, CVE-2021-33698, CVE-2021-38176, CVE-2021-38163, CVE-2021-37531, CVE-2021-33672, CVE-2021-38162, CVE-2021-38177, CVE-2021-33685, CVE-2021-38175, CVE-2021-38150, CVE-2021-33679, CVE-2021-38164, CVE-2021-33686, CVE-2021-21489, CVE-2021-33688, CVE-2021-37532, CVE-2021-38174

Code execution vulnerability in Nitro Pro PDF

Description	
Researchers from Cisco Talos has identified a code execution vulnerability in Nitro Pro PDF. The popular PDF modification application is vulnerable to a use-after-free vulnerability that can be triggered with malicious PDF once opened. The OEM has released a update to patch the vulnerabilities.	
Source	https://blog.talosintelligence.com/2021/09/nitro-pro-code-execution.html?&web_view=true
Infected Technology	Nitro Pro PDF
Recommendation	Apply the update released
CVE-ID	CVE-2021-21798

Legacy IBM System X Servers not getting patches for High-Severity Bug

Description	
According to Lenovo, two IBM System X models, namely IBM System x 3550 M3 and IBM System x 3650 M3 will not be getting any security patches for their command injection vulnerabilities as they were retired and software and security support for System x 3550 and 3650 ended on December 31, 2019. The bug allows malicious actors to execute arbitrary commands through a vulnerable application called integrated Management Module.	
Source	https://securityaffairs.co/wordpress/122330/security/amd-driver-vulnerability.html?web_view=true
Infected Technology	IBM System x 3550 M3 and IBM System x 3650 M3
Recommendation	Discontinue the use of the system | Disable SSH and Telnet Change the default Administrator password during initial configuration Enforce strong passwords Only grant access to trusted administrators
CVE-ID	CVE-2021-3723,

AMD addresses Vulnerability in PSP driver

Description	
AMD has issued PSP driver version 3.08.17.735 to fix a critical information disclosure vulnerability that allowed non-privileged users to read uninitialized physical memory pages, where the original data is either moved or paged out.	
Source	https://securityaffairs.co/wordpress/122330/security/amd-driver-vulnerability.html?web_view=true
Infected Technology	AMD Platform Security Processor Chipset Driver
Recommendation	Update driver version to 3.08.17.735 or later
CVE-ID	CVE-2021-26333

Google Releases security updates for Chrome Browser

Description	
Google has released updates for its web browser, “Google Chrome” addressing 11 security issues out of which, two are said to be actively exploited zero-days in the wild. The vulnerabilities address an out of bounds write in V8 JavaScript engine and a use after free flaw in Indexed DB API.	
Source	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html
Infected Technology	Google Chrome
Recommendation	Update chrome to the latest version
CVE-ID	CVE-2021-30632 CVE-2021-30633

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**

OUR SERVICES

Our services as information security company includes:


INFORMATION SECURITY AUDIT


VULNERABILITY ASSESSMENT


PENETRATION TESTING


MANAGED/CO.MANAGED SOC


INCIDENT RESPONSE


THREAT ANALYSIS


SERVER HARDENING


CYBER SECURITY CONSULTANT


INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/