April 05
2021

INFOSEC WEEKLY

#MADE4SECURITY

- Legacy QNAP NAS Devices Vulnerable to Zero-Day Attack
- VMware fixes bug allowing attackers to steal admin credentials
- Citrix Patches DoD Vulnerabilites in Hypervisor
- Reflected XSS Vulnerability In “Ivory Search” WP Plugin Impact Over 60K sites
- Windows OS Feature Used to Evade Firewall and Persistence Gain
- Fake jQuery file infects WordPress sites with malware

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.

1. Legacy QNAP NAS Devices Vulnerable to Zero-Day Attack

Description	
Some legacy models of QNAP network-attached storage devices are vulnerable to remote unauthenticated attacks because of two unpatched vulnerabilities. It affects legacy QNAP Systems storage hardware and exposes devices to remote unauthenticated attackers. The bugs impact QNAP's model TS-231 network-attached storage (NAS) hardware, allowing an attacker to manipulate stored data and hijack the device. The vulnerabilities also impact some non-legacy QNAP NAS gear. However, it is important to note that patches are available for non-legacy QNAP NAS hardware.	
Source	https://securingsam.com/new-vulnerabilities-allow-complete-takeover/
Infected Technology	Legacy and some non-legacy Models of QNAP NAS
CVE ID	CVE-2020-2509, CVE-2021-36195
Recommendation	Apply the patch for available product through OEM download center For legacy product, restrict the access to authorized user until patch is released.

2. VMware fixes bug allowing attackers to steal admin credentials

Description	
VMware has fixed a bug that allowed attackers to steal admin credentials. It was caused by a Server-Side Request Forgery bug in the vRealize Operations Manager API. Attackers can exploit the vulnerability remotely without requiring authentications or user interaction in low complexity attacks to steal administrative credentials. VMware rated the security flaw as high severity giving it a base score of 8.6 out of 10. VMware has also published workaround instructions for admins who don't want to or can't immediately patch servers running vulnerable vRealize Operations versions (e.g., there is no patch for their version).	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0004.html
Infected Technology	VMware vRealize Operations
CVE ID	CVE-2021-21975
Recommendation	Apply patches or follow the workaround instructions if a patch is unavailable.

3. Citrix Patches DoD Vulnerabilities in Hypervisor

Description

Citrix Hypervisor, an open-source platform for virtualization, has addressed vulnerabilities that could be abused to cause the host to crash or become unresponsive if the attacker can execute privileged code in a guest virtual machine. The two vulnerabilities were found to impact all currently supported Hypervisor versions. Among the two, the first vulnerability tracked as CVE-2021-28038 is identified in Linux Kernel through 5.11.3, as used with Xen PV, and exists because of the lack of the necessary treatment for errors in the netback drivers, leading to the host OS denial of service. Likewise, the second vulnerability tracked as CVE-2021-28688 was found to impact all Linux versions that include the fix for CVE-2021-26930 (xsa-365), a bug that impacts blkback's grant mapping. The new vulnerability could allow for a malicious frontend driver to cause resource leaks from a corresponding backend driver, thus leading to a denial of service on the host.

Source	https://support.citrix.com/article/CTX306565
Infected Technology	Citrix Hypervisor (up to and including 8.2 LTSR)
CVE ID	CVE-2021-28038, CVE-2021-28688
Recommendation	Consider installing the hotfixes and update to the patched versions.

4. Reflected XSS Vulnerability In "Ivory Search" WP Plugin Impact Over 60K sites

Description

On March 28, 2021, Astra Security Threat Intelligence Team responsibly disclosed a vulnerability in Ivory Search, a WordPress Search Plugin installed on over 60,000 sites. This security vulnerability could be exploited by an attacker to perform malicious actions on a victim's website. This is a medium severity reflected XSS vulnerability affecting Ivory search plugin version 4.6.0 and below. Therefore, if updated to its latest version containing the patch, 4.6.1, immediately could avoid its exploitation. Astra Security Suite – WordPress Firewall & Malware Scanner can help sites to secure against this vulnerability.

Source	https://www.getastra.com/blog/911/plugin-exploit/reflected-xss-vulnerability-in-ivory-search-wp-plugin/
Infected Technology	"Ivory Search" WP Plugin
Recommendation	Update to the latest version (4.6.1) or use Astra Security Suite.

5. Windows OS Feature Used to Evade Firewall and Persistence Gain

Description
Malicious actors have found ways to utilize Microsoft's Background Intelligent Transfer Service (BITS) for deploying malicious payloads on the Windows machine. The payloads are deployed in a stealth manner. BITS is commonly used for delivering OS updates and for fetching malicious signature updates by Windows Defender antivirus scanner. The malicious payloads would be used to create BITS jobs and upload and download files for the service host process. This process is integral for evading a firewall that usually blocks the malicious and unknown process. The leverage of the BITS service was used to create a 'System Update' job to trigger the KEGTAPP backdoor for HTTP transfer of the nonexistent files.

Source	https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
Infected Technology	Microsoft's Background Intelligent Transfer Service (BITS)

6. Fake jQuery file infects WordPress sites with malware

Description
Security researchers have spotted counterfeit versions of the jQuery Migrate plugin injected on dozens of websites that contain obfuscated code to load malware. These files are named jquery-migrate.js and jquery-migrate.min.js and present at the exact locations where JavaScript files are normally present on WordPress sites but are malicious. As of today, over 7.2 million websites use the jQuery Migrate plugin, which explains why attackers would disguise their malware under this popular plugin's name.

Source	https://www.bleepingcomputer.com/news/security/fake-jquery-files-infect-wordpress-sites-with-malware/?&web_view=true
Infected Technology	jQuery Migrate plugin
Recommendation	Consider performing security audits and checking for anomalies that may indicate signs of malicious activity before using any jQuery plugins

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/