July 25, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Atlassian patches batch of critical vulnerabilities across multiple products
- Microsoft Releases Fix for Zero-Day Flaw in July 2022 Security Patch Rollout
- Hackers Distributing Password Cracking Tool for PLCs and HMIs to Target Industrial Systems
- Patch released by SonicWall for critical SQLi vulnerability.
- Grafana patches vulnerability that could lead to admin account takeover

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.

Atlassian patches batch of critical vulnerabilities across multiple products

Description

A hardcore credential flaw in Questions for Confluence and servlet filter bypasses multiple other products has been addressed by Atlassian. Servlet filters were capable to intercept and process HTTP requests before a client request is sent to a backend resource, and from a backend resource before they are sent to a client. A vulnerability allowed an unauthenticated attacker to bypass servlet filters used by as-yet unspecified first-and third-party apps. An attacker could send a specially crafted HTTP request to bypass the servlet filter used to validate legitimate Atlassian Gadgets and achieve cross-site scripting (XSS).

Source	https://portswigger.net/daily-swig/atlassian-patches-batch-of-critical-vulnerabilities-across-multiple-products
Infected Technology	Atlassian
Recommendation	Update to latest version
CVE_ID	CVE-2022-26136, CVE-2022-26137, CVE-2022-26138

Microsoft Releases Fix for Zero-Day Flaw in July 2022 Security Patch Rollout

Description

Microsoft released its monthly Patch Tuesday updates to address 84 new security flaws spanning multiple product categories, counting a zero-day vulnerability under active attack in the wild. Four of the 84 flaws are classified as Critical, while the remaining 80 are classified as Important. Two more issues in the Chromium-based Edge browser were separately fixed by the tech giant, one of which closes yet another zero-day vulnerability that Google acknowledged was being actively used in real attacks. CVE-2022-22047 (CVSS score: 7.8), a scenario of privilege escalation in the Windows Client Server Runtime Subsystem (CSRSS) that might be exploited by an attacker to obtain SYSTEM permissions, is at the top of the list of this month's updates.

Source	https://thehackernews.com/2022/07/microsoft-releases-fix-for-zero-day.html
Infected Technology	Windows Client Server Runtime Subsystem Windows Network File System Windows Graphics Remote Procedure Call Runtime Windows Shell Microsoft Defender for Endpoint Internet Information Services Security Account Manager
Recommendation	Patch the latest update as soon as possible form the original vendor.
CVE_ID	CVE-2022-22047 CVE-2022-22029 CVE-2022-22039 CVE-2022-30221 CVE-2022-30222 CVE-2022-22038

Hackers Distributing Password Cracking Tool for PLCs and HMIs to Target Industrial Systems

Description

A new attack uses password cracking software to take control of Programmable Logic Controllers (PLCs) and convince the devices into joining a botnet, with industrial engineers and operators as its primary targets. To recover the password at will, the malware took advantage of a flaw in the firmware. The program was also a malware dropper, infecting the computer with the Sality virus and converting the host into a peer in the Sality peer-to-peer botnet. Sensitive information sent in cleartext at risk of information leakage and unauthorized alterations. In firmware version 2.72, which was published last month, the problem was fixed. It appears that this kind of software has an ecosystem. There are several websites and social media profiles that all advertise password crackers.

Source	https://thehackernews.com/2022/07/hackers-distributing-password-cracking.html
Infected Technology	Firmware version 2.72
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-2003

Patch released by SonicWall for critical SQLi vulnerability.

Description

SonicWall released a patch for a critical SQL injection (SQLi) vulnerability that affected its Analytics and (Global management system) GMS products. An authenticated user is able to exploit this weakness due to “improper neutralization of special elements”. H4lo and Catalpa from DBappSecurity HAT are credited for discovering this vulnerability. SonicWall states that “Likelihood of exploitation may significantly be reduced by incorporating a Web application firewall (WAF) to block SQLi attempts.

Source	https://thehackernews.com/2022/07/sonicwall-issues-patch-for-critical-bug.html
Infected Technology	Firmware version 2.72
Recommendation	• 2.5.0.3-2520 and earlier versions of Analytics On-Prem • GMS prior to and including 9.3.1-SP2-hotfix1 • Upgrade to Analytics 2.5.0.3-2520-Hotfix1 • Upgrade to GMS 9.3.1-SP2-Hostfic-2
CVE_ID	CVE-2022-22280

Grafana patches vulnerability that could lead to admin account takeover

Description

Open source analytics platform fixes bug that could lead to authentication bypass, privilege escalation. Malicious actors could take over an administrator account in Grafana due to a vulnerability in its OAuth login function, researchers have warned. The security flaw, tracked as CVE-2022-31107, could allow an attacker to access another user’s account on the open source analytics platform. Discovered by a team of researchers from HTTPVoid, the bug, which resides in the platform’s login function, “opens the door for attackers to elevate their privileges through cross-origin attacks against administrators on systems running vulnerable versions of the open source platform”.An attacker could therefore potentially gain access to an admin account.

Source	https://portswigger.net/daily-swig/grafana-patches-vulnerability-that-could-lead-to-admin-account-takeover
Infected Technology	Grafana
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-31107

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/