May 16, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft fixes more than 70 vulnerabilities
- Patch for critical OS command injection released for Zyxel firewall
- CISA Urges Organizations to Patch Actively Exploited F5 BIG-IP Vulnerability
- SonicWall Releases Patches for New Flaws Affecting SSLVPN SMA1000 Devices
- Icinga web vulnerabilities chained to hack IT monitoring software

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.

<table>
<tr><td colspan="2">Microsoft fixes more than 70 vulnerabilities</td></tr>
<tr><td colspan="2"><b>Description</b></td></tr>
<tr><td colspan="2">Microsoft returned to its normal monthly patching volume in May, disclosing and fixing 74 vulnerabilities as part of the company’s latest security update. This month’s Patch Tuesday includes seven critical vulnerabilities after Microsoft disclosed more than 140 security issues in April. The point-to-point tunneling feature in Windows contains two of the most serious vulnerabilities that could allow an attacker to execute remote code on a targeted RAS server machine. While CVE-2022-21972 and CVE-2022-23270 are rated “critical,” Microsoft stated the attack complexity is high since an adversary needs to win a race condition, making it less likely an attacker could exploit these issues. CVE-2022-26931 and CVE-2022-26923 are elevation of privilege vulnerabilities in Windows Kerberos and Windows Active Directory, respectively. They both are considered critical, though CVE-2022-26931 is considered less likely to be exploited because it has a higher attack complexity.</td></tr>
<tr><td>Source</td><td>https://blog.talosintelligence.com/2022/05/microsoft-patch-tuesday-for-may-2022.html</td></tr>
<tr><td>Infected Technology</td><td>RAS server machine, Windows Kerberos and Windows Active Directory, Windows self-hosted integration runtime service</td></tr>
<tr><td>Recommendation</td><td>Update to latest version</td></tr>
<tr><td>CVE_ID</td><td>CVE-2022-29104, CVE-2022-29108, CVE-2022-29114, CVE-2022-29132, CVE-2022-29142, CVE-2022-23279</td></tr>
</table>

Patch for critical OS command injection released for Zyxel firewall

Description

Rapid7, a Cybersecurity firm, discovered and reported a command injection in April 13, 2020. This vulnerability enabled an unauthenticated user to gain remote code execution (RCE) in Zyxel devices. Zyxel said, “A command injection vulnerability in the CGI program of some firewall versions could allow an attacker to modify specific files and then execute some OS commands on a vulnerable device.” According to Rapid7, there are approximately 16,213 vulnerable devices exposed to the internet, making it a high value target for hackers.

Source	https://thehackernews.com/2022/05/zyxel-releases-patch-for-critical.html
Infected Technology	USG FLEX 100(W), 200, 500, 700, USG FLEX 50(W) / USG20(W)-VPN, ATP series, VPN series, VMG3312-T20A
Recommendation	Update to patch version ZLD V5.30 immediately.
CVE_ID	CVE-2022-30525, CVE-2022-30525, CVE-2022-30525, CVE-2022-30525

SonicWall Releases Patches for New Flaws Affecting SSLVPN SMA1000 Devices

Description

SonicWall has issued a security alert for its Secure Mobile Access (SMA) 1000 equipment, which has a high-severity authentication bypass vulnerability. SMA 6200, 6210, 7200, 7210, 8000v running firmware versions 12.4.0 and 12.4.1 are affected by the flaws. An attacker might get unauthorized access to internal resources and potentially lead potential victims to malicious websites if the above issues are successfully exploited. The issues do not impact SMA 1000 series operating versions before to 12.4.0, SMA 100 series, Central Management Servers (CMS), or remote access clients, according to SonicWall. Vulnerability with CVSS score is CVSS score: 8.2 Unauthenticated Access Control Bypass, CVSS score: 6.1 URL redirection to an untrusted site (open redirection), CVSS score Use of a shared and hard-coded cryptographic key.

Source	https://thehackernews.com/2022/05/sonicwall-releases-patches-for-new.html
Infected Technology	SMA 6200, 6210, 7200, 7210, 8000v running firmware versions 12.4.0 and 12.4.1
Recommendation	Update patches as soon as its updated
CVE_ID	CVE-2022-22282, CVE-2022-1702, CVE-2022-1701

CISA Urges Organizations to Patch Actively Exploited F5 BIG-IP Vulnerability

Description

Following indications of active misuse in the wild, CISA has added the recently reported F5 BIG-IP bug to its Known Exploited Vulnerabilities CatLog. The issue, which has a CVSS score of 9.8, is a major weakness in the BIG-IP iControl REST endpoint that allows an unauthenticated attacker to run arbitrary system commands. On the susceptible server, an attacker may utilize this vulnerability to do almost whatever they want. This involves making modifications to the target network's configuration, stealing sensitive information, and moving laterally within the network. To make matters worse, evidence has surfaced that the remote code execution weakness is being exploited to recursively destroy all files on targeted servers by using the "rm -rf /*" command. Given that the web server runs as root, every susceptible server should be taken care of, as well as any vulnerable BIG-IP equipment.

Source	https://thehackernews.com/2022/05/cisa-urges-organizations-to-patch.html
Infected Technology	F5 BIG-IP
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-1388

Icinga web vulnerabilities chained to hack IT monitoring software

Description

Unauthenticated attackers might run arbitrary PHP code and hijack computers thanks to a pair of vulnerabilities in the online control panel of IT monitoring system Icinga. Two path traversal vulnerabilities and a weakness that allows arbitrary PHP code to be executed from the administrator interface were recently addressed web-related vulnerabilities uncovered by security researchers at SonarSource. CVE-2022-24716 is a path traversal bug in Icinga Web 2 and CVE-2022-24715 is a separate path traversal bug that also exploits behavior of PHP validating a SSH key by using a NULL byte. The PHP vulnerability is in the OpenSSL core extension.

Source	https://portswigger.net/daily-swig/brace-of-icinga-web-vulnerabilities-easily-chained-to-hack-it-monitoring-software
Infected Technology	Icinga Web versions below 2.8.6, 2.9.6 and 2.10
Recommendation	Update to latest version
CVE_ID	CVE-2022-24716, CVE-2022-24715

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/