March 22, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft releases one-click mitigation tool for Exchange Server hacks
- Cisco Plugs Security Hole in Small Business Routers
- Hackers are exploiting a server vulnerability with a severity of 9.8 out of 10
- The Linux kernel bugs that surfaced after 15 years
- Zoom Screen-Sharing Glitch leaks sensitive data ‘briefly’
- Popular WordPress plugins vulnerable to arbitrary code execution
- DuckDuckGo browser extension vulnerability leaves Edge users open to potential cyber-snooping
- Computer giant Acer hit by $50 million ransomware attack

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. Microsoft releases one-click mitigation tool for Exchange Server hacks

Description

Microsoft has released a one-click mitigation tool namely "Microsoft Exchange On-Premises Mitigation Tool" as a stopgap for IT admins. The tool has been designed to help customers that might not have security or IT staff on hand. It is important to note that the tool is not an alternative to patching but should be considered a means to mitigate the risk of exploitation until the update has been applied. Although the tool has been tested across Exchange Server 2013, 2016, and 2019, however, it can also be run on any existing Exchange servers. Despite the tool also includes Microsoft Safety Scanner and URL rewrite mitigation for CVE-2021-26855, which can lead to remote code execution (RCE) attacks if exploited.

Source	https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/
Infected Technology	Microsoft Exchange Servers
CVE ID	CVE-2021-26855
Recommendation	Consider patching Exchange servers.

2. Cisco Plugs Security Hole in Small Business Routers

Description

A popular line of small business routers made by Cisco Systems is vulnerable to a high-severity vulnerability. If exploited, the flaw could allow a remote – albeit authenticated – attacker to execute code or restart affected devices unexpectedly. Cisco issued fixes on Wednesday for the flaw in its RV132W ADSL2+ Wireless-N VPN routers and RV134W VDSL2 Wireless-AC VPN routers. These routers are described by Cisco as "networking-in-a-box" models that are targeted for small or home offices and smaller deployments. The vulnerability stems from an issue in the routers' web-based management interface. It ranks 7.2 out of 10 on the CVSS scale, making it high severity.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p
Infected Technology	• RV132W ADSL2+ Wireless-N VPN routers • RV134W VDSL2 Wireless-AC VPN routers
CVE ID	CVE-2021-1287
Recommendation	Consider applying security patches provided by cisco.

3. Hackers are exploiting a server vulnerability with a severity of 9.8 out of 10

Description

In a development security pro feared, attackers are actively targeting yet another set of critical server vulnerabilities that leave corporations and governments open to serious network intrusions. The vulnerability this time is in BIG-IP, a line of server appliances sold by Seattle-based F5 Networks. Last week, F5 disclosed and patched critical BIG-IP vulnerabilities that allow hackers to gain complete control of a server. Despite a severity rating of 9.8 out of 10, the security flaws got overshadowed by a different set of critical vulnerabilities. The severity in part is because the vulnerabilities require limited skill to exploit. But more importantly, once attackers have control of a BIG-IP server, they are inside the security perimeter of the network using it. That means attackers can quickly access other sensitive parts of the network.

Source	https://arstechnica.com/gadgets/2021/03/to-security-pros-dread-another-critical-server-vulnerability-is-under-exploit/
Infected Technology	BIG-IP
CVE-ID	CVE-2021-22986
Recommendation	Update and patch the vulnerability

4. The Linux kernel bugs that surfaced after 15 years

Description

A trio of security holes was found by security company GRIMM researchers in an almost forgotten corner of the mainline Linux Kernel. The first two of which have a Common Vulnerability Scoring System (CVSS) score above 7, which is high. Today, the bugs are still around. One of them could even be used in a Local Privilege Escalation attack. Although the vulnerable SCSI or iSCSI drive code isn't loaded by default on most desktop, if your server needs RDMA (Remote Direct Memory Access), a high-throughput, low-latency networking technology, it's likely to autoload the rdma-core Linux kernel module, which brings with it the vulnerable SCSI code.

Source	https://github.com/grimm-co/NotQuite0DayFriday/tree/trunk/2021.03.12-linux-iscsi
Infected Technology	CentOS 8, Red Hat Enterprise Linux (RHEL) 8, Fedora, SUSE Linux Enterprise Server (SLES), Ubuntu <= 18.8
CVE ID	CVE-2021-27365, CVE-2021-27363, CVE-2021-27364
Recommendation	Consider patching your Linux operating system.

5. Zoom Screen-Sharing Glitch leaks sensitive data 'briefly'

Description

A glitch has been identified in Zoom's screen sharing feature that shows parts of the screen that the presenter did not intend to share. This glitch results in leaking user's data that has not been intended to, however, for a brief amount of time. The glitch occurs while operating in a split application window. The issue arises in a situation when the user operates Zoom on split windows while opening other applications in the background. The application in the non-shared mode can be perceived and the contents within that application can be read by the meeting participants for a brief moment. This glitch is most vulnerable in a situation where the participants record the meeting session and can view the recording to potentially gain access to sensitive data.

Source	https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-044.txt
Infected Technology	Zoom 5.4.3 and 5.5.4
CVE ID	CVE-2021-28133
Recommendation	Install the latest patches and update to the latest version.

6. Popular WordPress plugins vulnerable to arbitrary code execution

Description

Two popular WordPress plugins are found to be faulty that impacts over 7 million websites. Elementor and WP Super Cache contain multiple undisclosed vulnerabilities that lead an attacker to run arbitrary codes. The successful exploitation of the vulnerabilities could lead to the possibility of a website takeover in some scenarios. A set of stored cross-site scripting (XSS) vulnerabilities was identified in Elementor due to the lack of HTML tag validation on the server-side hence, letting the attackers execute malicious JavaScript through a crafted request. WP Super Cache plugin was identified to contain an authenticated remote code execution (RCE) vulnerability. The successful exploitation could lead the attackers to upload and execute malicious code with the motive to gain control of the site.

Source	https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/ https://patchstack.com/database/vulnerability/wp-super-cache/wordpress-wp-super-cache-plugin-1-7-1-authenticated-remote-code-execution-rce-vulnerability
Infected Technology	Elementor < 3.1.2 and WP Super Cache <=1.7.1
Recommendation	Update plugins to the latest versions

7. DuckDuckGo browser extension vulnerability leaves Edge users open to potential cyber-snooping

Description

DuckDuckGo has fixed a universal cross-site scripting (uXSS) flaw in a popular browser extension for Chrome and Firefox. The vulnerability was discovered in DuckDuckGo Privacy Essentials, which blocks hidden trackers and offers private browsing features. It could be leveraged to achieve uXSS on victims' devices, revealed researcher Wladimir Palant, meaning that arbitrary code could be executed on any domain. While it has been patched in Chrome and, since the time of writing, in Mozilla Firefox, no update has been issued for other browsers such as Microsoft Edge. The security flaw could enable malicious actors to spy on all websites that the user is visiting, leaving sensitive information such as banking details and other data potentially accessible. The attackers can spy on anything the users do in their browser, they can manipulate displayed information, take over accounts, impersonate the user.

Source	https://palant.info/2021/03/15/duckduckgo-privacy-essentials-vulnerabilities-insecure-communication-and-universal-xss/
Infected Technology	All Web Browsers
Recommendation	Update your browser to its latest version.

8. Computer giant Acer hit by $50 million ransomware attack

Description	
Taiwanese electronics and computer maker company "Acer", well-known for laptops, desktops, and monitors has been hit by a REvil ransomware attack where the threat actors are demanding the largest known ransom to date, $50,000,000. the ransomware gang announced on their data leak site that they had breached Acer and shared some images of allegedly stolen files as proof. These leaked images are for documents that include financial spreadsheets, bank balances, and bank communications. Advanced Intel's Andariel cyber intelligence platform detected that the Revil gang recently targeted a Microsoft Exchange server on Acer's domain. "Advanced Intel's Andariel cyberintelligence system detected that one particular REvil affiliate pursued Microsoft Exchange weaponization.	
Source	https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/
Infected Technology	Acer Technologies

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/