October 3, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- L2 Network Security Control Bypass Flaws Impact Multiple Cisco Products
- CISA: Hackers exploit critical Bitbucket Server flaw in attacks
- Vulnerabilities in popular library affect Unix-based devices
- New Unpatched Microsoft Exchange Zero-Day Under Active Exploitation
- Heap based buffer overflow vulnerability in WhatsApp

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.

L2 Network Security Control Bypass Flaws Impact Multiple Cisco Products

Description

Cisco this week has confirmed that tens of its enterprise routers and switches are impacted by bypass vulnerabilities in the Layer-2 (L2) network security controls. A total of four medium-severity security issues were found in the L2 network security controls, in the Ethernet encapsulation protocols, the CERT Coordination Center (CERT/CC) at the Carnegie Mellon University notes in an advisory. The bugs allow for stacking of virtual local area network (VLAN) headers and 802.2 LLC/SNAP headers, enabling an attacker to bypass a device's various filtering capabilities, including IPv6 RA Guard, Dynamic ARP inspection, and IPv6 Neighbor Discovery (ND) protection. CERT/CC says that more than 200 vendors have been warned of these vulnerabilities, but that only two of them have confirmed impact, namely Cisco and Juniper Networks.

Source	https://www.securityweek.com/l2-network-security-control-bypass-flaws-impact-multiple-cisco-products
Infected Technology	Cisco Layer 2 network packet inspection functionality
Recommendation	Update the latest patch released.
CVE_ID	CVE-2021-27853 CVE-2021-27854 CVE-2021-27861 CVE-2021-27862

CISA: Hackers exploit critical Bitbucket Server flaw in attacks

Description

Three more security flaws has been added by the Cybersecurity and Infrastructure Security Agency (CISA) to its list of bugs exploited in attacks, including a Bit bucket Server RCE and two Microsoft Exchange zero-days. The third security flaws is a critical command injection vulnerability in Atlassian's Bitbucket Server and Data Center, with publicly available proof of concept exploited code where attacker can gain remote execution by exploiting the flaw via malicious HTTP requests. This RCE vulnerability impacts all Bitbucket Server and Data Center versions after 6.10.17, including 7.0.0 and up to 8.3.0.

Source	https://www.bleepingcomputer.com/news/security/cisa-hackers-exploit-critical-bitbucket-server-flaw-in-attacks/
Infected Technology	Bitbucket Server
Recommendation	Update the latest patch released by CISA
CVE_ID	CVE-2022-41082 CVE-2022-41040 CVE-2022-36804

Vulnerabilities in popular library affect Unix-based devices

Description

Cisco Talos recently discovered a memory corruption vulnerability in the uClibC library that could affect any Unix-based devices that use this library. uClibC and uClibC-ng are lightweight replacements for the popular gLibc library, which is the GNU Project's implementation of the C standard library. CVE-2022-29503 and CVE-2022-29504 are memory corruption vulnerabilities in uClibC and uClibc-ng that can occur if a malicious user repeatedly creates threads. Many embedded devices utilize this library, but Talos specifically confirmed that the Anker Eufy Homebase 2, version 2.1.8.8h, is affected by this vulnerability.

Source	https://talosintelligence.com/vulnerability_reports/TALOS-2022-1517
Infected Technology	uClibC LIbrary
Recommendation	Update the latest patch releasedby CISA

New Unpatched Microsoft Exchange Zero-Day Under Active Exploitation

Description

The two flaws are officially still waiting to receive CVE numbers, however the Zero Day Initiative is tracking them as ZDI-CAN-18333 and ZDI-CAN-18802. Adversaries might drop web shells and make lateral network moves if the vulnerabilities were exploited successfully, giving them access to the victim's systems. The majority of the obfuscated web shells discovered are being dropped to Exchange servers. The attacker employs Antsword, an active cross-platform open-source application with Chinese roots that allows online shell control, using the user-agent. .According to GTSC, exploit requests for the ProxyShell Exchange Server issues show in IIS logs in a similar way. The targeted servers had previously been patched against the flaws, however.

Source	https://www.gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html
Infected Technology	Microsoft Exchange

Heap based buffer overflow vulnerability in WhatsApp

Description	
Two remote code execution flaws were resolved by WhatsApp. These might have given an attacker the ability to control a gadget remotely and send commands. In WhatsApp, an integer overflow could lead to remote code execution (RCE) during a connected video call. When an integer value is given a value that is too large to fit in the reserved representation that can be represented with a specific number of digits, this is known as an integer overflow. This is typically greater than the maximum, but it is also possible for it to be less than the minimum representable number. An attacker might leverage the ability to remotely execute code by overwriting other areas of the system's memory by writing a larger value into the memory.	
Source	https://www.whatsapp.com/security/advisories/2022/?lang=en
Infected Technology	whatsapp
Recommendation	Update the latest patch available.

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