March 29 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Cisco fixes Jabber client bug in Windows and macOS
- OpenSSL fixes certificate validation and severe DOS vulnerabilities
- Another Critical RCE Flaw Discovered in SolarWinds Orion Platform
- Active Exploits Hit WordPress Sites Vulnerable to Thrive, Themes Flaws
- Apple fixes an iOS zero-day vulnerability actively used in attacks
- Microsoft fixes Windows PSExec privilege elevation vulnerability
- Microsoft Exchange servers now targeted by Black Kingdom ransomware

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. Cisco fixes Jabber client bug in Windows and macOS

Description	
Cisco has rectified critical arbitrary program execution vulnerability in several versions of Cisco Jabber client software. The vulnerability impacts various operating system versions that include Windows, macOS, Android, and iOS. The vulnerability resides due to an improper input validation of the incoming message's contents. The attackers were required to be authenticated in the XMPP server for using the vulnerable software to craft malicious XMPP messages. The successful exploitation of this vulnerability does not require user authentication enables remote attackers to execute arbitrary programs on the devices running the unpatched software hence, enabling arbitrary code execution.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-jabber-PWrTATTC
Infected Technology	Cisco Jabber for Windows, macOS, Android, or iOS, versions 12.9 or earlier
CVE ID	CVE-2021-1411, CVE-2021-1417, CVE-2021-1418, CVE-2021-1469, CVE-2021-1471
Recommendation	Consider installing the latest version of Cisco Jabber.

2. OpenSSL fixes certificate validation and severe DOS vulnerabilities

Description	
OpenSSL project has solved two high-severity vulnerabilities present in the OpenSSL products. The vulnerabilities include the Denial of Service (DoS) flaw and improper certificate authority (CA) certification validation. The DOS attack was possible to the Null pointer dereferencing flaw. The DoS vulnerability (CVE rated) was present only in the OpenSSL server instances. The vulnerability in the OpenSSL TLS server caused the server to crash during renegotiation as a result of a malicious ClientHello message. The certification validation vulnerability was present due to an error in the implementation of the check. The failed OpenSSL instances while checking the non-CA certificated opened up the possibility of an attacker exploiting this vulnerability.	
Source	https://www.openssl.org/news/secadv/20210325.txt
Infected Technology	OpenSSL version 1.1.1-1.1.1j (both inclusive)
CVE ID	CVE-2021-3449, CVE-2021-3450
Recommendation	Update to OpenSSL 1.1.1k

3. Another Critical RCE Flaw Discovered in SolarWinds Orion Platform

Description	
IT infrastructure management provider SolarWinds on Thursday released a new update to its Orion networking monitoring tool with fixes for four security vulnerabilities. The first one is the JSON deserialization flaw that allows an authenticated user to execute arbitrary code through the test alert actions feature available in Orion Web Console. The second one is the vulnerability that could be leveraged by an adversary to achieve RCE in the Orion Job Scheduler. The third one includes a high-severity stored cross-site scripting (XSS) vulnerability in the "add custom tab" within the customize view page and the other last one being tabnabbing and open redirect vulnerability in the custom menu item option page. The update also brings some security improvements, with fixes for preventing XSS attacks and enabling UAC protection for Orion database managers, among others.	
Source	https://documentation.solarwinds.com/en/Success_Center/orionplatform/Content/Release_Notes/Orion_Platform_2020-2-5_release_notes.htm
Infected Technology	Orion Platform version < 2020.2.5
CVE ID	CVE-2020-35856, CVE-2021-3109
Recommendation	Consider updating to the latest release i.e. Orion Platform 2020.2.5.

4. Active Exploits Hit WordPress Sites Vulnerable to Thrive, Themes Flaws

Description	
Thrive Themes has recently patched vulnerabilities in its WordPress plugins and legacy Themes – but attackers are targeting those who haven't yet applied security updates. Two vulnerabilities were discovered across both these Legacy Themes and plugins, and patches were subsequently released on March 12. The flaws could be chained together to allow unauthenticated attackers to ultimately upload arbitrary files on vulnerable WordPress sites – allowing for website compromise. However, researchers warn that more than 100,000 WordPress sites using Thrive Themes products may still be vulnerable.	
Source	https://www.wordfence.com/blog/2021/03/recently-patched-vulnerability-in-thrive-themes-actively-exploited-in-the-wild/
Infected Technology	WordPress Sites
Recommendation	Apply the released security patch

5. Apple fixes an iOS zero-day vulnerability actively used in attacks

Description	
Apple has released security updates to address an iOS zero-day bug actively exploited in the wild and affecting iPhone, iPad, iPod, and Apple Watch devices. The zero-day was discovered in the Webkit browser engine and allows attackers to launch universal cross-site scripting attacks after tricking targets into opening maliciously crafted web content on their devices. The zero-days were addressed by Apple on March 26, 2021, by improving the management of object lifetimes in iOS 15.4.2, iOS 12.5.2, and watchOS 7.3.3. As put by Apple, the latest update provides important security updates and is recommended for all users.	
Source	About the security content of iOS 14.4.2 and iPadOS 14.4.2 - Apple Support
Infected Technology	iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation), iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, iPod touch (6th generation), Apple Watch Series 3 and later
CVE ID	CVE-2021-1879
Recommendation	Consider updating your Apple devices to the latest iOS version.

6. Microsoft fixes Windows PSExec privilege elevation vulnerability

Description	
Microsoft has fixed a vulnerability in the PsExec utility that allows local users to gain elevated privileges on Windows devices. PsExec is a Sysinternals utility designed to allow administrators to perform various activities on remote computers, such as launching executables and displaying the output on the local computer or creating reverse shells. Due to the tool's versatility, threat actors commonly use PsExec in their post-exploitation toolkits to spread laterally to other machines on a network, execute commands on a large number of devices simultaneously, or deploy malware such as ransomware.	
Source	https://docs.microsoft.com/en-us/sysinternals/downloads/psexec
Infected Technology	PsExec utility
Recommendation	Consider updating PsExec utility to the latest version

7. Microsoft Exchange servers now targeted by Black Kingdom ransomware

Description	
Another ransomware operation is known as 'Black Kingdom' is exploiting the Microsoft Exchange Server ProxyLogon vulnerabilities to encrypt servers. Over the weekend, the threat actor was compromising Microsoft Exchange Server ProxyLogon vulnerabilities to encrypt servers. Based on the logs from his honeypots, security researcher Marcus Hutchins states that the threat actor used the vulnerability to execute a PowerShell script that downloads the ransomware executable from 'yuuuuu44[.]com' and then pushes it out to other computers on the network. The ransom notes demand $10,000 in bitcoin and use the Bitcoin address (1Lf8ZzcEhhRiXpk6YNQFpCJcUisiXb34FT) for payment.	
Source	https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-now-targeted-by-black-kingdom-ransomware/
Infected Technology	Microsoft Exchange servers
Recommendation	Consider keeping the sensitive information in an encrypted format.

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/