March 8, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft releases multiple security updates for Exchange Server
- A new Chrome 0-day bug under active attack
- Qualys gets breached using Accellion Exploit
- Researchers Found 3 New Malware Strains Used by SolarWinds Hackers
- Several Cisco Products Exposed to DoS Attacks Due to Snort Vulnerability
- GRUB2 boot loader reveals multiple high severity vulnerabilities
- VMware Patches Remote Code Execution Vulnerability in View Planner
- Minion privilege escalation exploit patched in SaltStack Salt project

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 multiple security updates for Exchange Server

Description	
Microsoft has released several security updates for Microsoft Exchange Server to address vulnerabilities that have been used in limited targeted attacks. Due to the critical nature of these vulnerabilities, Microsoft recommends customers apply the updates to affected systems immediately to protect against these exploits and to prevent future abuse across the ecosystem. These vulnerabilities are used as part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443. The vulnerabilities affect Microsoft Exchange Server. However, Exchange Online is not affected.	
Source	https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
Infected Technology	• Microsoft Exchange Server 2013 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2019
CVE ID	CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 CVE-2021-27065
Recommendation	• Consider installing the security updates provided by Microsoft. • Consider restricting untrusted connections to the Exchange Server. • Consider setting up a VPN to separate the Exchange server from external access.

2. A new Chrome 0-day bug under active attack

Description	
Google has released the latest Chrome update (Chrome 89.0.4389.72) for Windows, MAC, and Linux on 2nd March 2021. The update rectifies various zero-day vulnerabilities and a total of 47 security fixes including a severe concern called 'object lifecycle issue in audio'. Google has acknowledged the exploit for the vulnerability exists but has not shared information relating to the specifics about the vulnerability and it's working. Google has also issued a fix for another actively exploited heap buffer overflow. This vulnerability is present in the V8 JavaScript rendering engine of Google Chrome.	
Source	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html
Infected Technology	Google Chrome
CVE ID	CVE-2021-21166, CVE-2021-21148
Recommendation	Consider updating Google Chrome to its latest version.

3. Qualys gets breached using Accellion Exploit

Description	
A cloud security firm, Qualys, has been vulnerable to a data breach as a result of zero-day vulnerabilities in the Accellion File Transfer Appliance (FTA) server. The endpoint was exploited to extract sensitive business documents. The detailed probe from the Qualys Security Team identified unauthorized access to the file in the Accellion FTA servers. The servers were located in a De-Militarized Zone (DMZ) which is separated from the rest of the internal network infrastructure. The unauthorized access did not impact the service or the access to the customers using Qualys however, a limited number of customers were vulnerable to this unauthorized access.	
Source	https://blog.qualys.com/vulnerabilities-research/2021/03/03/qualys-update-on-accellion-fta-security-incident
Infected Technology	Qualys Cloud Platform
CVE ID	CVE-2021-27730, CVE-2021-27731

4. Researchers Found 3 New Malware Strains Used by SolarWinds Hackers

Description	
On Thursday, FireEye and Microsoft said that they discovered three more malware strains in connection with the SolarWinds supply-chain attack, including a sophisticated second-stage backdoor. The identified malware strains were Dubbed GoldMax (aka SUNSHUTTLE), GoldFinder, and Sibot. According to Microsoft, these tools are new pieces of malware that are unique to this actor which are tailor-made for specific networks and are addressed to be introduced after the actor has gained access through compromised credentials or the SolarWinds binary. Alongside, the capabilities of these malware strains differ from previously known NOBELIUM tools and attack patterns and reiterate the actor's sophistication.	
Source	https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
Infected Technology	SolarWinds

5. Several Cisco Products Exposed to DoS Attacks Due to Snort Vulnerability

Description	
Multiple Cisco products are affected by a vulnerability in the Ethernet Frame Decoder of the Snort detection engine that could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper handling of error conditions when processing Ethernet frames. An attacker could exploit this vulnerability by sending malicious Ethernet frames through an affected device. A successful exploit could allow the attacker to exhaust disk space on the affected device, which could result in administrators being unable to log in to the device or the device being unable to boot up correctly.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n
Infected Technology	Snort detection engine version < 2.9.17.
CVE ID	CVE-2021-1285
Recommendation	Consider installing the security updates provided by cisco.

6. GRUB2 boot loader reveals multiple high severity vulnerabilities

Description	
GRUB, a popular boot loader used by Unix-based operating systems has fixed multiple high severity vulnerabilities. This week GRUB project maintainers have released hundreds of upstream patches for the severe boot loader flaws like Incomplete List of Disallowed Inputs, Use-after-free, Out-of-bound write, Stack buffer overflow, Improper Authorization, etc. These flaws could allow the ACPI command which allowed a privileged user to load crafted ACPI tables when Secure Boot is enabled. They also allowed an attacker to unload a module used as a dependency without checking if any other dependent module is still loaded and allowed a privileged user to remove memory regions when Secure Boot is enabled.	
Source	https://git.savannah.gnu.org/gitweb/?p=grub.git;a=shortlog
Infected Technology	GRUB2 Boot Loader
CVE ID	CVE-2020-14372, CVE-2020-25632, CVE-2020-25647, CVE-2020-27749, CVE-2020-27779, CVE-2021-3418, CVE-2021-20225, CVE-2021-20233
Recommendation	Consider installing the security patches provided by respective distros and vendors.

7. VMware Patches Remote Code Execution Vulnerability in View Planner

Description	
VMware this week announced the availability of a security patch for VMware View Planner, to address a vulnerability leading to remote code execution. VMware explains that the bug is rooted in improper input validation, complemented by lack of authorization. Together, these issues could be abused for the upload of arbitrary files in the logupload web application, which could then lead to code execution. According to the company, an attacker looking to exploit this bug needs to have already compromised the network to access View Planner Harness. The attacker could then abuse the vulnerability to upload a specially crafted file and then execute it, which would essentially result in the execution of code remotely, within the logupload container.	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0003.html
Infected Technology	VMware
CVE ID	CVE 2021-21978
Recommendation	Consider applying the security patch provided by VMware.

8. Minion privilege escalation exploit patched in SaltStack Salt project

Description	
The vulnerability is described as a privilege escalation bug impacting SaltStack Salt minions allowing “an unprivileged user to create files in any non-blacklisted directory through a command injection in a process named”. Salt includes a master system and minions, of which the latter facilitates commands sent to the master, and both often run as root. A command injection vulnerability in minions when the master system summons a process called restart check. Exploits can be triggered if attackers use crafted process names, permitting local users to escalate their privileges on the root – if they can create files on a minion in a non-forbidden directory. The vulnerability as put by investigators may also be responsible to perform container escapes, including performing the exploit.	
Source	https://saltproject.io/security_announcements/active-saltstack-cve-release-2021-feb-25/
Infected Technology	Salt version <3002.5
CVE ID	CVE-2020-28243
Recommendation	Consider upgrading to the patched versions (version >3002.5)

9. Vendor Quickly Patches Serious Vulnerability in NATO-Approved Firewall	
Description	
A critical vulnerability discovered in a firewall appliance made by Germany-based cybersecurity company Genua could be useful to treat actors once they've gained access to an organization's network. Genua claims that its Genugate firewall is the only one in the world to receive a "highly resistant" rating from the government and says it's compliant with NATO's "NATO Restricted" requirements from data protection. However, SEC Consult on Monday revealed that the Genugate firewall is affected by a critical authentication bypass vulnerability in the product's administration interface. An attacker who has network access to an administration interface can exploit the vulnerability to log in to the device's admin panel, which enables reconfiguration of the whole firewall, such as firewall ruleset, email filtering configuration, web application firewall settings, proxy settings, etc.	
Source	https://sec-consult.com/vulnerability-lab/advisory/authentication-bypass-genua-genugate/
Infected Technology	GenuGate <0.1 p4, <9.6 p7, <9.0/9.0 Z p19
CVE ID	CVE-2021-27215
Recommendation	Consider upgrading the firewall appliances to their patched versions as listed below: • GenuGate 10.1 p4(G1010_004), • GenuGate 9.6 P7(G960_007), • GenuGate 9.0 and 9.0 Z p19 (G900_019)

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**