

October 11, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- New Python ransomware targets virtual machines, ESXi hypervisors to encrypt
- Google patches Four Severe Vulnerabilities in chrome
- Gatekeeper Bypass for macOS
- Multiple Critical Flaws Discovered in Honeywell Experion PKS and ACE Controllers
- Unauthenticated remote access vulnerability on Dahua cams remains unpatched



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.

New Python ransomware targets virtual machines, ESXi hypervisors to encrypt

Description

Researchers have discovered a new Python ransomware from an unnamed gang that's striking ESXi servers and virtual machines (VMs) with what they called "sniper-like" speed. The ransomware is being used to compromise and encrypt VMs hosted on an ESXi hypervisor in operations that, soup-to-nuts, are taking less than three hours to complete from initial breach to encryption. This is one of the fastest ransomware attacks appeared to precision-target the ESXi platform. It's rare to see the Python coding language used for ransomware. that Python comes pre-installed on Linux-based systems such as ESXi, and thus makes Python-based attacks possible on these systems.

Source <https://news.sophos.com/en-us/2021/10/05/python-ransomware-script-targets-esxi-server-for-encryption/>

Infected Technology ESXi

Recommendation

1. Limit ESXi access
2. Used named users and least privilege
3. Minimize the number of open ESXi firewall ports
4. Automate ESXi host management
5. Take advantage of lockdown mode
6. Check VIB package integrity
7. Consider ESXi account lockout

Google patches Four Severe Vulnerabilities in chrome

Description

Google has warned of reports that a zero-day vulnerability in the chrome browser is being actively exploited in the wild. The flaw, described as a user-free bug in Garbage Collection, the browser also address two heaper buffer overflow vulnerabilities. Attackers could exploit these vulnerabilities through specially crafted webpages to compromise a visitor's system and potentially execute code in the context of the browser. Google says the Chrome extended stable channel too was updated to version 94.0.4606.81 for Windows and Mac.

Source https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html

Infected Technology Google Chrome

Recommendation Update the latest available patch

CVE_ID CVE-2021-37977, CVE-2021-37978, CVE-2021-37979, CVE-2021-37980

Gatekeeper Bypass for macOS

Description

A new vulnerability on macOS can lead to bypass of all three protections that Apple implemented against malicious file downloads, namely file quarantine, Gatekeeper, notarization. The issue is found in the Archive Utility component of macOS Big Sur and Catalina and can be exploited using a specially crafted ZIP file. This can assist attacker could execute unsigned binaries on macOS devices, even with Gatekeeper enforcing code signatures without being alerted to the malicious code execution.

| | |
|--------|---|
| Source | https://labs.f-secure.com/blog/the-discovery-of-cve-2021-1810/ |
|--------|---|

| | |
|---------------------|----------------------------|
| Infected Technology | macOS Big Sur and Catalina |
|---------------------|----------------------------|

| | |
|----------------|--|
| Recommendation | Update latest release of macOS Big Sur 11.3 and Security Update 2021-002 for Catalina. |
|----------------|--|

| | |
|-----|---------------|
| CVE | CVE-2021-1810 |
|-----|---------------|

Multiple Critical Flaws Discovered in Honeywell Experion PKS and ACE Controllers

Description

On Tuesday there were multiple security vulnerabilities issued by CISA affecting all versions of Honeywell Experion Process Knowledge System C200, C200E, C300, and ACE controllers that could be exploited to achieve remote code execution and denial-of-service (DoS) conditions. The issues is on the download code procedure that's essential to program the logical running in the controller which enables the attacker to copy the process and upload arbitrary CLL binary files

| | |
|--------|---|
| Source | https://www.claroty.com/2021/10/05/blog-research-target-dcs-finding-fixing-critical-bugs-in-honeywell-experion-pks/ |
|--------|---|

| | |
|---------------------|--|
| Infected Technology | Honeywell Experion PKS and ACE controllers |
|---------------------|--|

| | |
|----------------|---|
| Recommendation | Apply patches as soon as possible in order to mitigate these vulnerabilities fully. |
|----------------|---|

| | |
|-----|--|
| CVE | CVE-2021-38397, CVE-2021-38395, CVE-2021-38399 |
|-----|--|

Unauthenticated remote access vulnerability on Dahua cams remains unpatched

Description

Two authenticated bypass vulnerabilities for Dahua cameras have a proof-of-concept exploit made public. The two remotely exploitable attack can be performed during the login process by sending specially crafter data packets to the target device.

| | |
|--------|---|
| Source | https://www.dahuasecurity.com/support/cybersecurity/details/957 |
|--------|---|

| | |
|---------------------|------------|
| Infected Technology | Dahua Cams |
|---------------------|------------|

| | |
|----------------|--|
| Recommendation | Upgrade the cameras to latest firmware and update to a stronger password |
|----------------|--|

| | |
|--------|-----------------------------------|
| CVE-ID | CVE-2021-33044 and CVE-2021-33045 |
|--------|-----------------------------------|

Yamale Python Package affected with Code Execution bug

Description

Researchers have discovered high severity code injection vulnerability in 23andMe's Yamale to execute arbitrary Python code. Attacker can manipulate the file schema file provided as input to the tool and achieve code execution. The package has been reportedly used by more than 200 repositories on GitHub.

| | |
|--------|---|
| Source | https://nvd.nist.gov/vuln/detail/CVE-2021-38305 |
|--------|---|

| | |
|---------------------|----------------------|
| Infected Technology | Yamale version 3.0.8 |
|---------------------|----------------------|

| | |
|----------------|---|
| Recommendation | Patch update the Yamale 23andMe to latest |
|----------------|---|

| | |
|--------|----------------|
| CVE-ID | CVE-2021-38305 |
|--------|----------------|

Apache puts forth emergency updates addressing exploited bug

Description

Apache has released HTTP Web server 2.4.51 addressing the shortcomings of a previously released security update. The flaw allowed perpetrators to view contents of file stored on a vulnerable server. Also, if the mod_cgi module was loaded and the default "Require all denied" option was missing, the vulnerability could be used for RCE.

| | |
|--------|---|
| Source | https://www.bleepingcomputer.com/news/security/apache-emergency-update-fixes-incomplete-patch-for-exploited-bug/?&web_view=true |
|--------|---|

| | |
|---------------------|--------------------|
| Infected Technology | Apache HTTP Server |
|---------------------|--------------------|

| | |
|----------------|---------------------------------------|
| Recommendation | Upgrade servers to Apache HTTP 2.4.51 |
|----------------|---------------------------------------|

| | |
|--------|----------------------------------|
| CVE-ID | CVE-2021-41773 CVE-2021-42013 |
|--------|----------------------------------|

Huawei cloud targeted by threat actors

Description

News about new cloud service providers being targeted with cryptocurrency-mining malware and cryptojacking attacks have surfaced. Perpetrators deploy code that nulls the applications and services in the Huawei cloud. Apache has released HTTP Web server 2.4.51 addressing the shortcomings of a previously released security update. The flaw allowed perpetrators to view contents of file stored on a vulnerable server. Also, if the mod_cgi module was loaded and the default "Require all denied" option was missing, the vulnerability could be used for RCE.

| | |
|--------|---|
| Source | https://www.bleepingcomputer.com/news/security/apache-emergency-update-fixes-incomplete-patch-for-exploited-bug/?&web_view=true |
|--------|---|

| | |
|---------------------|--------------------|
| Infected Technology | Apache HTTP Server |
|---------------------|--------------------|

| | |
|----------------|---------------------------------------|
| Recommendation | Upgrade servers to Apache HTTP 2.4.51 |
|----------------|---------------------------------------|

| | |
|--------|----------------------------------|
| CVE-ID | CVE-2021-41773 CVE-2021-42013 |
|--------|----------------------------------|

For any queries/recommendations:

Contact us: [whois@cryptogen**nepal**.com](mailto: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/>