

November 22, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Chrome 96 plugs High-Risk Browser Flaws
- Microsoft fixes reflected XSS in Exchange Server
- Netgear fixes code execution flaw in many SOHO devices
- Security flaw on six million Sky routers
- CKEditor vulnerabilities addressed
- Malicious Python packages caught stealing Discord tokens, installing shells



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.

Chrome 96 plugs High-Risk Browser Flaws

Description

Google is releasing Chrome 96 for Windows, Mac, and Linux this week, which addresses 25 security flaws, including three high-severity bugs that bad actors might exploit to attack users. The Chrome team announce the elevation of Chrome 96 to the stable channel for Windows, Mac, and Linux. Chrome has been updated with 25 security patches, including 18 reported by external researchers. Seven of these are deemed high-severity issues, thus it's critical to upgrade as soon as feasible.

Source	https://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html
--------	---

Infected Technology	Chrome
---------------------	--------

Recommendation	Update the latest available patch
----------------	-----------------------------------

Microsoft fixes reflected XSS in Exchange Server

Description

Microsoft has patched an Exchange Server reflected cross-site scripting (XSS) vulnerability. It was just another XSS; an attacker could have manipulated the DOM and exploited it to read/send emails, phish, do application state-changing activities, and so on.

Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41349
--------	---

Infected Technology	Microsoft Exchange Server
---------------------	---------------------------

Recommendation	Update the latest available patch.
----------------	------------------------------------

CVE_ID	CVE-2021-41349
--------	----------------

Netgear fixes code execution flaw in many SOHO devices

Description

Netgear fixed a pre-authentication buffer overflow problem in its small office/home office (SOHO) devices, which could be exploited by an attacker on a local area network (LAN) to remotely execute malware with root capabilities. The issue is located in the device's Universal Plug-and-Play (UPnP) upnpd daemon routines linked to the handling of "unauthenticated HTTP SUBSCRIBE and UNSUBSCRIBE requests from clients that desire to receive updates whenever the network's UPnP configuration changes."

Source	https://kb.netgear.com/000064361/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Multiple-Products-PSV-2021-0168
--------	---

Recommendation	Update the latest available patch.
----------------	------------------------------------

CVE_ID	CVE-2021-34991
--------	----------------

Security flaw on six million Sky routers

Description

Sky Broadband had an underlying DNS rebinding vulnerability affecting about 6 million customers through their routers. The flaw affected customers using default admin password on their routers. Any non-default credentials could have been brute forced. The exploit allows attackers to reconfigure a victim's home router that could lead to stolen passwords for banking and other sensitive sites.

Source	https://threatpost.com/6m-sky-routers-exposed-18-months/176483/
--------	---

Infected technology	<ul style="list-style-type: none">• Sky Hub 3 (ER110)• Sky Hub 3.5 (ER115)• Booster 3 (EE120)• Sky Hub (SR101)• Sky Hub 4 (SR203)• Booster 4 (SE210)
---------------------	---

Recommendation	Updates have been provided to the affected models
----------------	---

CKEditor vulnerabilities addressed

Description

Drupal, a widely used web content management system (CMS), has released security updates for its CKEditor. “Moderately Critical” pair of cross-site scripting (XSS) bugs may impact numerous online applications. The XSS vulnerabilities could enable attackers to inject malformed HTML bypassing content sanitization, which could result in executing JavaScript code.

Source	https://portswigger.net/daily-swig/ckeditor-vulnerabilities-pose-xss-threat-to-drupal-and-other-downstream-applications?&web_view=true
--------	---

Infected Technology	CKEditor
---------------------	----------

Recommendation	Update the release to 4.17.0, Update Drupal 9.2 to 9.2.9, 9.1 to 9.1.14, 8.9 to 8.9.20.
----------------	---

CVE-ID	CVE-2021-33829
--------	----------------

Malicious Python packages caught stealing Discord tokens, installing shells

Description

A many as 11 malicious Python packages have been cumulatively download more than 41000 times from Python Package Index (PyPI) repository which could be exploited to steal Discord access tokens, passwords and stage dependency confusion attacks. The list and the description of the Packages can be viewed via the Source link.

Source	https://therecord.media/malicious-python-packages-caught-stealing-discord-tokens-installing-shells/?web_view=true
--------	---

Infected Technology	Python Libraries
---------------------	------------------

High-Severity Vulnerability in Azure AD

Description

When a new automation account is set up in Azure, due to a misconfiguration in the Azure, Automation Account “Run as” credentials, it ends up being stored in clear text in the Azure AD and can be accessed by anyone with access to the information on app registrations. The bug can be exploited to escalate privileges to contributor of any subscription that has an automation account and access the resources in the affected subscriptions including the credentials stored in the key vaults and any sensitive information in the Azure services. Also, the resources can be deleted, and the azure tenants can be taken offline.

Source	https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-cloud-vulnerability-credmanifest/
--------	---

Infected Technology	Azure AD, Azure Automation self-signed certificates
---------------------	---

Recommendation	Azure AD customers should cycle through all Automation Account “Run as” certificates to make sure no credentials are exposed.
----------------	---

CVE-ID	CVE-2021-42306 (CVSS score of 8.1)
--------	------------------------------------

Thousands of Firefox users accidentally commit login cookies on GitHub

Description

GitHub projects presently host thousands of Firefox cookie databases containing sensitive data that might possibly be exploited to hijack authorized sessions. These cookies.sqlite databases are often located in a user's Firefox profiles folder and are used to store cookies across browser sessions. When committing work and sending it to their public GitHub projects, the impacted individuals unintentionally uploaded their own cookies.sqlite database.

Source	https://www.theregister.com/2021/11/18/firefox_cookies_github/?&web_view=true
--------	---

Infected Technology	Github
---------------------	--------

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/>