September 28, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Google Chrome Bugs open browsers to attack
- Microsoft Windows XP Source code leaked online
- Fortinet VPN with default setting leaves businesses open to attackers
- Instagram Bug could let attacker remote access to phone
- Microsoft Bing Server exposed user's search query and location
- 29 High-Severity Bugs patched by CISCO
- Privilege Escalation Vulnerability patched by Google on their Cloud Service

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. Google Chrome Bugs open browsers to attack

Description

Google has released a new version of its browser for Mac, Windows and Linux which fix 10 security flaws. The update addressed a buffer overflow flaw and insufficient policy enforcement. The buffer overflow flaw allowed attacker to perform out of band memory access via specially crafted HTML page. Three insufficient policy management for extensions allowing malicious extensions to escape the sandbox via Chrome Extension. There is no proof of the vulnerabilities being exploited in the wild however Google has urged to update the browser to the latest release.

Source	https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop_21.html
Infected Technology	Google Chrome
CVE	CVE-2020-15960, CVE-2020-15961, CVE-2020-15962, CVE-2020-15963, CVE-2020-15965, CVE-2020-15966, CVE-2020-15964
Recommendation	Update to the latest stable version 85.0.4183.121

2. Microsoft Windows XP Source code leaked online

Description

Source code of Microsoft Windows XP along with several older operating system has been leaked with a torrent file weighing 43 GB in total. The leaked file is also said to include the source code for Windows Server 2003. Besides older operating system, the leak also contains components of Windows 10 and first Operating system for Xbox. Microsoft has ended the support for XP in 2014. Along with the source code of Operating Systems, a media folder related to conspiracy theory about Bill Gates has been released with the torrent file.

Source	https://thehackernews.com/2020/09/windows-xp-source-code.html
Infected Technology	Windows XP, 2000; CE 3; CE 4; CE 5; Embedded 7; Embedded CE; NT 3.5, NT 4; MS-DOS 3.30, MS-DOS 6.0
Recommendation	Update to the Operating System currently supported by OEM

3. Fortinet VPN with default setting leaves businesses open to attackers

Description

During the pandemic, businesses have opted for work for home for their employees. According to a report, over 200,000 businesses have deployed FortiGate VPN solution with default configuration. With the default configuration, the employees are now vulnerable to Man-in-the-middle attack. The VPN-Client only verifies the SSL issuer to be FortiGate allowing attacker to use SSL for different router and rerouting the traffic to perform MITM attack.

Source	https://securingsam.com/breaching-the-fort/
Infected Technology	FortiGate VPN
Recommendation	Change the default certificate provided by Fortinet Out of the box

4. Instagram Bug could let attacker remote access to phone

Description

A critical vulnerability disclosed by Check Point Researcher in Instagram's Android application could have let remote attacker to take over target device by sending a specially crafted image. The vulnerability in the application not only allowed attacker to manipulate the application action such as spy on victim's account and trigger action on behalf of victim but also execute arbitrary code on the device. The vulnerability is due to memory corruption vulnerability that leads to remote code execution.

Source	https://blog.checkpoint.com/2020/09/24/instahack-how-researchers-were-able-to-take-over-the-instagram-app-using-a-malicious-image/
Infected Technology	Instagram for Android (128.0.0.26.128 and before)
CVE	CVE-2020-1895
Recommendation	Update the application to the latest version

5. Microsoft Bing Server exposed user’s search query and location

Description

A back-end server of Microsoft Bing exposed search queries, device details, GPS location of mobile application users. The data was available for any one to download without any authentication via a cache of log files worth 6.5 TB. The server required authentication until September 10 and was addressed on September 16. While the data did not contain name and addresses, deviceID, devicehash and Advertising Id assigned by Microsoft was included in the leaked file.

Source	https://www.wizcase.com/blog/bing-leak-research/
Infected Technology	Microsoft Bing

6. 29 High-Severity Bugs patched by CISCO

Description

Cisco has released many patches aimed at fixing bugs in the networking giant’s ubiquitous IOS operating system. The patches plug holes in a wide range of products and address denial-of-service, file overwrite and input validation attacks. Along with 29 high severity rated bugs, they also released patches with 13 medium severity vulnerabilities. Among those vulnerabilities some flaws were tied to a flaw in Cisco's Zone-Based Firewalls while some impacted any Cisco hardware running Cisco IOS XE's software and authenticated local attacker to execute arbitrary code.

Source	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir&limit=50#~Vulnerabilities
Infected Technology	Cisco Devices
CVE	CVE-2020-3421 CVE-2020-3480 CVE-2020-3417 CVE-2020-3418 CVE-2020-3509 CVE-2020-3559
Recommendation	Cisco has released patch updates to address the vulnerabilities

7. Privilege Escalation Vulnerability patched by Google on their Cloud Service

Description	

Google recently issued a patch update for a Privilege Escalation Vulnerability in OS Config, a Google Cloud Platform service for Compute Engine that is designed for managing operating systems running on virtual machine instances. OS Config service API and agent allow users to perform various tasks across a group of VM instances, including applying patches, collecting and reviewing OS information, and installing, removing and updating software packages. Exploitation of the vulnerability required access to the targeted system with a low-privileged shell to exploit this vulnerability.

Source	https://github.com/irsl/google-osconfig-privesc
Infected Technology	Google Cloud Service
Recommendation	Upgrade OS package to the fixed version release after 2020-09-05

For any queries/recommendations:

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