July 06, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Critical flaw in F5 BIG-IP Application security servers
- Ransomware targeting macOS users via pirated apps
- Critical Apache Guacamole flaw puts remote desktops at risk
- Microsoft releases urgent windows update to patch two critical flaws
- Cisco Talos disclosed technical details of Chrome and Firefox
- .NET Core vulnerability allows attackers to evade malware detection
- Cisco warns of high severity bugs in Small business switches

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. Critical flaw in F5 BIG-IP Application security servers

Description	
Cybersecurity researchers today issued a security advisory warning enterprises and governments across the globe to immediately patch a highly-critical remote code execution vulnerability affecting F5's BIG-IP networking devices running application security servers. The vulnerability, assigned CVE-2020-5902 and rated as critical with a CVSS score of 10 out of 10, could let remote attackers take complete control of the targeted systems, eventually gaining surveillance over the application data they manage. This vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the TMUI, through the BIG-IP management port and/or Self IPs, to execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code. This vulnerability may result in complete system compromise. The BIG-IP system in Appliance mode is also vulnerable.	
Source	https://support.f5.com/csp/article/K52145254
Infected Technology	BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, LLC, PEM); Version 15.x, 14.x, 13.x, 12.x, 11.x
CVEs	CVE-2020-5902, CVE-2020-5903
Recommendation	Immediately Update to Hot Fix issued by F5 (15.1.0.4, 14.1.2.6, 13.1.3.4, 12.1.5.2, 11.6.5.2)

2. Ransomware targeting macOS users via pirated apps

Description	
Researchers from K7 lab have discovered a ransomware variant dubbed "EvilQuest" – packaged alongside legitimate application appearing to be Google subject update or Apple's CrashReporter. The trojan beside encrypting data in infected device also act as key logger, creates reverse shell to gain persistence and steal cryptocurrency wallet-related files. The trojan confirms the installation is not under any debugger and detects sandboxed environment. The trojan's features is beside a typical ransomware and allows attacker to remotely execute command in victim's system and kill any security software that may detect its presence in the system	
Source	https://thehackernews.com/2020/07/macos-ransomware-attack.html
Infected Technology	MacOS
Recommendation	Do not installed applications from unknown sources Keep backup of the critical files

3. Critical Apache Guacamole flaw puts remote desktops at risk

Description	
A research published by Check Point Research uncovered multiple critical reverse RDP vulnerabilities in Apache Guacamole, remote desktop application, which allowed attackers to take full control over Guacamole server, intercept and control all other connected sessions. The attack can be executed via a compromised system inside the corporate network. Guacamole server has added the support for FreeRDP which also contained RCE. The flaw has been addressed via patch on June.	
Source	https://thehackernews.com/2020/07/apache-guacamole-hacking.html
Infected Platform	Guacamole Server
Recommendation	Update the server to the latest version Use security tools to protect remote communication

4. Microsoft releases urgent windows update to patch two critical flaws

Description	
Microsoft has released an out-of-band software update to patch two high-risk vulnerabilities in Windows 10 devices and Server editions. The flaw resides in the way Microsoft codec library handles objects in memory. The vulnerability could allow remote code execution in the infected devices that could compromise the machine. The attack is executed when the user clicks on specially crafted image using any app utilizing built-in Windows codec Library.	
Source	https://thehackernews.com/2020/07/windows-security-update.html
Infected Technology	Windows 10 version: 1709, 1803, 1809, 1903, 1909, 2004; Windows server 2019, Windows Server version: 1803, 1903, 1909, 2004
CVEs	CVE-2020-1425, CVE-2020-1457
Recommendation	Implement the patch released via Windows update.

5. Cisco Talos disclosed technical details of Chrome and Firefox

Description	
Cisco Talos has disclosed technical details of recently patched vulnerabilities of Chrome and Firefox web browsers. A memory corruption vulnerability in PDFium, open source PDF library used by Google chrome and other application, allowed attacker to execute arbitrary code in browser by tricking victim to open document injected with JavaScript code. The vulnerability had score of 8.8 in CVSS score. Another vulnerability defined in advisory is in Firefox's URL mPath functionality resulted in sensitive information disclosure which can help an attacker to bypass ASLR and excute arbitrary code in browser's context.	
Source	https://securityaffairs.co/wordpress/105547/security/talos-chrome-firefox-flaws.html
Infected Technology	Google Chrome and Mozilla Firefox
Recommendation	Update to the latest version

6. .NET Core vulnerability allows attackers to evade malware detection

Description	
A vulnerability in .NET Core library allowed malicious program to evade malware detection. The flaw is caused due to Path Traversal in the library that allowed malicious garbage collection DLLs to be loaded by low-privilege users. The flaw is present in latest version of .NET framework with no fix available. The attacker, however, requires access to the victim's device prior to set environmental variable due to which Microsoft does not consider it as security issue.	
Source	https://www.bleepingcomputer.com/news/security/net-core-vulnerability-lets-attackers-evade-malware-detection/
Infected Technology	.NET Framework 3.1.x
Recommendation	Monitor for environmental variable named "COMPlus_GCName"

7. Cisco warns of high severity bugs in Small business switches

Description	
Cisco has released a warning of high-severity bugs in dozens of its small business switches. The vulnerability allows remote, unauthenticated attacker to access the switches' Management interface with administrative privilege. Cisco 250 Series Smart Switches, Cisco 350 Series Managed switches and 350X and 550X series stackable managed switches, Small Business 200 Series Smart Switches, Small Business 300 Series Managed Switches and Small Business 500 Series Stackable Managed Switches are affected, and no public exploitation has been reported. Software updates with patch are available for the devices except those reaching EOL. The flaw, CVE-2020-3297, with score of 8.1 in CVSS scale allowed attacker to determine current session identifier through brute force and reuse it to takeover current session.	
Source	https://threatpost.com/cisco-warns-high-severity-bug-small-business-switch/157090/?web_view=true
Infected Technology	Cisco 250 Series Smart Switches, Cisco 350 Series Managed switches and 350X and 550X series stackable managed switches, Small Business 200 Series Smart Switches, Small Business 300 Series Managed Switches and Small Business 500 Series Stackable Managed Switches
CVE	CVE-2020-3297
Recommendation	Apply the patch update released by Cisco Change the device, if affected, reaching End of Life

For any queries/recommendations:

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