November 21, 2022

# INFOSEC WEEKLY

#MADE4SECURITY

- QBot Phishing abuses Windows Control Panel EXE to infect devices
- Google Roulette: Developer console trick can trigger XSS in Chromium browsers
- Log4Shell-like code execution hole in popular Backstage Dev tool
- PCspooF: New Vulnerability Affects Networking Tech Used by Spacecraft and Aircraft
- Researchers Discover Hundreds of Amazon RDS Instances Leaking Users' Personal Data

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.

## QBot Phishing abuses Windows Control Panel EXE to infect devices

| **Description** | |
|---|---|
| The QBot malware are misusing the DLL hijacking flaw in the Windows 10 operating system's control panel that infects and can attempt to bypass threat detection by any security software. The malware is distributed through phishing emails. The threat actor creates a malicious DLL file with the same name as the program's DLL dependencies and store it in the same directory. When the program is executed, it would load the malicious DLL and infect the windows system. Abusing the Control Panel, the attack uses DLL hijacking flaw as the QBot installs malware from a trusted program like Windows 10 Control Panel which may not be flagged by security software and defender allowing it to evade detection. Furthermore, the threat actor can install Brute Ratel and Cobalt Strike for post-exploitation to gain remote access to corporate networks which can lead to corporate data theft and ransomware attacks. | |
| Source | https://www.bleepingcomputer.com/news/security/qbot-phishing-abuses-windows-control-panel-exe-to-infect-devices/ |
| Infected Technology | Windows 10 Operating System |
| Recommendation | Aware users about QBot Phishing Email and do not download any suspicious files. |

## Google Roulette: Developer console trick can trigger XSS in Chromium browsers

| Description | |
|---|---|
| Malicious actors can execute cross-site scripting (XSS) assaults across the subdomains of a website if they can deceive users of Chromium browsers into submitting a simple JavaScript command in the developer console. This is according to the results of security researcher Michał Bentkowski who detailed his findings in a blog post published yesterday (November 16) titled Google Roulette.While the flaw is hard to exploit and Google has opted not to repair it, it is an intriguing case study on the complexity of browser security. | |
| Source | https://portswigger.net/daily-swig/google-roulette-developer-console-trick-can-trigger-xss-in-chromium-browsers |
| Infected Technology | Chromium browsers |
| Recommendation | • Organization-wide awareness<br>• Content Security Policies (CSP) |

## Log4Shell-like code execution hole in popular Backstage Dev tool

| Description | |
|---|---|
| The Oxeye research team has been able to gain remote code execution in spotify's open source, CNCF- incubated project- Backstage, by exploiting a VM sandbox escape through vm2 third-party library. An unauthenticated threat actor can execute arbitrary system commands on a backstage application by exploiting a VM2 sandbox escape in the scaffolder core plugin. They reported this RCE vulnerability via spotify's bug bounty program, and the backstage team responded rapidly by patching it in version 1.5.1 and ranking the vulnerability with CVSS score of 9.8. | |
| Source | https://nakedsecurity.sophos.com/2022/11/15/log4shell-like-code-execution-hole-in-popular-backstage-dev-tool/ |
| Infected Technology | Backstage (Developer portal platform) |
| Recommendation | • Update to the latest version of the system as soon as possible.<br>• Sanitize your logging inputs and outputs |
| CVE_ID | CVE-2022-36067 |

| PCspooF: New Vulnerability Affects Networking Tech Used by Spacecraft and Aircraft | |
|---|---|
| **Description** | |
| The security guarantees made by TTE may be compromised by a fundamental networking technology vulnerability discovered by researchers from the University of Michigan and NASA. TTE is one of the networking technologies that make up a mixed-criticality network. The TTE devices will start to regularly lose sync and reconnect once the attack begins. Time-sensitive signals will gradually be lost or delayed because of this failure, causing systems to act in an unexpected and potentially dangerous way. This is achieved by injecting electromagnetic interference (EMI) into a TTE switch over an Ethernet connection, tricking the switch into delivering synchronization signals that appear to be real (i.e., protocol control frames or PCFs), and getting other TTE devices to accept them. | |
| Source | https://thehackernews.com/2022/11/pcspoof-new-vulnerability-affects.html |
| Infected Technology | TTE (Time-triggered ethernet) |
| Recommendation | • Using Optocouplers or surge protectors to block electromagnetic interference<br>• using a link-layer authentication protocol like IEEE 802.1AE<br>• increasing the number of sync masters<br>• disabling dangerous state transitions |

## Researchers Discover Hundreds of Amazon RDS Instances Leaking Users' Personal Data

**Description**

Mitiga, a cloud incident response company, discovered hundreds of databases on Amazon Relational Database Service exposing personal identifiable information. The personal information includes names, email addresses, phone numbers, dates of birth, marital status, car rental information and even company logins. The leak is result of a feature called public RDS snapshots, which allows for creating a backup of the entire database environment which can be accessed by all AWS accounts. The stolen data could be used for financial gain or leverage it to get a better grasp of a company's IT environment for secret intelligence gathering.

| | |
|---|---|
| Source | https://thehackernews.com/2022/11/researchers-discover-hundreds-of-amazon.html |
| Infected Technology | Amazon |
| Recommendation | • Not include private information when sharing snapshot as public and encrypt snapshots where applicable |

## High Severity Vulnerabilities Reported in F5 BIG-IP and BIG-IQ Devices

**Description**

F5 BIG-IP and BIG-IQ devices contain several security flaws that, if successfully exploited, might entirely compromise the vulnerable systems. The vulnerabilities might be exploited to get remote access to the devices and could gain persistent root access to the device's management interface. If such a situation occurred, a malicious party with access to the appliance's Advanced Shell (bash) may use these flaws as a weapon to run arbitrary system commands, add or remove files, or turn off services.

| | |
|---|---|
| Source | https://thehackernews.com/2022/11/high-severity-vulnerabilities-reported.html/ |
| Infected Technology | F5 BIG-IP and BIG-IQ devices |
| Recommendation | Users should apply the necessary "engineering hotfix" released by the company to mitigate potential risks. |
| CVE_ID | CVE-2022-41622<br>CVE-2022-41800<br>CVE-2022-41622 |

## RCE Flaw in Spotify's Backstage Software Catalog and Developer Platform

| **Description** | |
|---|---|
| A vulnerability in Spotify's Backstage has been discovered that can be exploited to gain remote code execution. The vulnerability takes advantage of critical sandbox escape in vm2, a well-known JavaScript sandbox library (CVE-2022-36067, aka Sandbreak). Threat actors can execute arbitrary system commands on Backstage application by exploiting vm2 sandbox escape in Scaffolder core plugin. | |
| Source | https://thehackernews.com/2022/11/critical-rce-flaw-reported-in-spotifys.html |
| Infected Technology | Software using Backstage Software Catalog and Developer Platform |
| Recommendation | Update to the latest version of Backstage |

## Exploit released for actively abused ProxyNotShell Exchange bug

| **Description** | |
|---|---|
| Proof-of-concept exploit code has been released online for two actively exploited and high-severity vulnerabilities in Microsoft Exchange, collectively known as ProxyNotShell. The two bugs, identified as CVE-2022-41082 and CVE-2022-41040, affect Microsoft Exchange Server 2013, 2016, and 2019 and give hackers access to elevated privileges that let them run PowerShell in the context of the system and execute arbitrary or remote code on compromised servers. Microsoft released security updates to address the two security flaws as part of the November 2022 Patch Tuesday, even though ProxyNotShell attacks have been detected since at least September 2022. | |
| Source | https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-abused-proxynotshell-exchange-bug/ |
| Infected Technology | Microsoft Exchange Server 2013,2016 and 2019 |
| Recommendation | Update Exchange Servers as soon as possible |
| CVE_ID | CVE-2022-41082<br>CVE-2022-41040 |

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/