# August 24, 2020

# INFOSEC WEEKLY

## #MADE4SECURITY

- Critical Jenkins Server Vulnerability Could leak Sensitive Information
- Fileless P2P Botnet Malware Targeting SSH Server Worldwide
- Job Offers Hackers
- Google Drive Flaw Could let Attackers trick you into installing Malware
- Flaw in IBM DB2 leaks sensitive information or cause Denial of Service
- Microsoft fixed two-year-old vulnerability actively exploited
- 8.3 Million records stolen in Freepik data breach
- Google fixed major bug allowing attacker to send spoofed emails

## 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 Jenkins Server Vulnerability Could leak Sensitive Information

| Description | |
|---|---|
| Jenkins- a popular open-source automation server software published an advisory on concerning a critical vulnerability in the jetty Web server that could result in memory corruption and cause confidential information to be disclosed. The flaw has a CVSS rating of 9.4 and impacts Eclipse jetty a full featured tool that provides a Java HTTP server and web container for use in software frameworks. The vulnerability may allow unauthenticated attackers to obtain HTTP response headers that may include sensitive data intended for another user. The flaw impacts Jetty and Jenkins Core, which added a mechanism to handle large HTTP response headers and prevent buffer overflows. | |
| Source | https://www.jenkins.io/security/advisory/2020-08-17/ |
| Infected Technology | Jetty Web Server version 9.4.27 to version 9.4.29 |
| CVE | CVE-2019-17638 |
| Recommendation | Update software to latest version to mitigate the buffer corruption flaw |

## 2. Fileless P2P Botnet Malware Targeting SSH Server Worldwide

| Description | |
|---|---|
| A peer-to-peer botnet called FritzFrog has hopped onto the scene, and actively breaching SSH servers. SSH Servers are pieces of software found in routers and IoT devices, among other machines, and they use the secure shell protocol to accept connections from remote computers. FritzFrog executes a worm malware is a modular, multi-threaded and fileless, leaving no trace on the infected machine's disk. Once the server is compromised, the malware creates a backdoor in the form pf an SSH public key, enabling the attackers ongoing access to victims' machines. | |
| Source | https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/ |
| Infected Technology | SSH Server |
| Recommendation | • Change SSH port<br>• Disable SSH access to FritzFrog if the service is not in use |

### 3. Job Offers Hackers

| Description | |
|---|---|
| Cyber security researcher observed as an increased in malicious cyber activity targeting the Aerospace & Defense Industry. Researcher discovered a series of malicious documents containing job postings taken from leading defense contractors to be used as lures. These malicious documents are intended to be sent to victims in order to install a data gathering implant. To achieve this , attackers first identify high-value targets, perform extensive research on their social and professional networks , and then pose as recruiters to send malicious documents loaded with the malware, masquerading as job advertisement and offerings | |
| Source | https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a |
| Recommendation | • Disable File download from private email account to company machines employee is connected to company network<br>• Examine the communication between desktop office Software and external server |

### 4. Google Drive Flaw Could let Attackers trick you into installing Malware

| Description | |
|---|---|
| The security bug is said to be the 'manage versions' feature offered by Google Drive that allows users to upload and manage different version of file. The feature allows users to upload and manage different version of a file. The Hackers may trick Google Drive users into downloading malware. The unpatched security loophole in Google drive could be misused by hackers to distribute malicious files disguised as legitimate documents or images. The loophole can be used by cybercriminals to launch spear phishing attack. This may lead to them sharing their confidential information or other dangerous software getting installed secretly in device | |
| Source | https://thehackernews.com/2020/08/google-drive-file-versions.html |
| Infected Technology | Google Drive |
| Recommendation | Observe Closely to Suspicious email and Drive notification to mitigate risk. |

### 5. Flaw in IBM DB2 leaks sensitive information or cause Denial of Service

| Description | |
|---|---|
| A memory leak vulnerability in IBM Db2 relational database could allow attacker to access sensitive data or cause denial of service (DOS). Db2 database for Windows, Linux and UNIX are affected with the vulnerability caused by improper usage of shared memory. The issue is due to lack of access protection in shared memory used by IBM Db2 trace facility allowing attacker with local access to gain read and write access. Incorrect data over targeted memory area could also allow attacker to cause DoS of the function. Researcher from Trustwave has informed the flaw could allow attacker to steal sensitive data and use it to expand their attack surface. | |
| Source | https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/ibm-db2-shared-memory-vulnerability-cve-2020-4414/ |
| Infected Technology | IBM Db2 for Windows, Linux and UNIX version: 9.7, 10.1, 10.5, 11.1, 11.5 |
| CVE | CVE-2020-4414 |
| Recommendation | Apply the patch released for the mentioned CVE |

### 6. Microsoft fixed two-year-old vulnerability actively exploited

| Description | |
|---|---|
| Microsoft has fixed a vulnerability that allowed MSI files to be converted to Malicious Java executables while retaining a legitimate company's digital signature. The vulnerability had been reported 2 years ago, which was originally not planned for a fix. The fix removes the digital signature of MSI if they have been tampered by JAR file appended to it. The flaw was present due to how Windows reads MSI file for signature discarding the rest of the contents once end of MSI signature is reached. | |
| Source | https://medium.com/@TalBeerySec/glueball-the-story-of-cve-2020-1464-50091a1f98bd |
| Infected Technology | Windows |
| CVE | CVE-2020-1464 |
| Recommendation | Apply the patch released by Microsoft |

## 7. 8.3 Million records stolen in Freepik data breach

| Description | |
|---|---|
| Freepik, a company with largest online graphic resource site and icon database, faced a data breach where attacker stole user's email and available password hashes of 8.3 Million users. 4.5 Million out of the breached account had logged into the platform with 0-auth via Google, Facebook and Twitter resulting in leakage of email id while the rest of the user's email address and hashed password has been stolen in the breach. Freepik has reset the password of the affected users and sent the mail to the users to initiate a new password. | |
| Source | https://www.freepik.com/blog/statement-on-security-incident-at-freepik-company/ |
| Infected Technology | Freepik and Flaticon |
| Recommendation | Reset the password of the platform<br>Change matching credentials used in any other platform |

## 8. Google fixed major bug allowing attacker to send spoofed emails

| Description | |
|---|---|
| Google fixed a critical bug that allowed attacker to send spoofed malicious email to Google user or enterprise customer. The flaw resided due to missing verification in mail routes that could pass SPF and DMARC. The attack abuses the broken recipient issue in Google's mail validation rules. The victim, if using Gmail or G Suite, pass the SPF and DMARC as the email will be sent from Google's backend. The spoofed email also is unlikely to be filtered and had lower spam score. Google patched the issue within 7 hours of the report getting published. | |
| Source | https://ezh.es/blog/2020/08/the-confused-mailman-sending-spf-and-dmarc-passing-mail-as-any-gmail-or-g-suite-customer/ |
| Infected Technology | Gmail and G Suite |

For any queries/recommendations:

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