

July 4,  
2022

# INFOSEC WEEKLY

#MADE4SECURITY

- Critical RCE bug in patched in latest Gitlab security release
- UnRAR path traversal flaw can lead to RCE in Zimbra
- Active Exploitation of 'PwnKit' Linux Vulnerability in the Wild
- Vulnerability in Amazon Photos Android App Exposed User Information
- Firefox 102 Patches 19 Vulnerabilities, Improves Privacy



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.

---

## Critical RCE bug in patched in latest Gitlab security release

### Description

Gitlab has addressed a serious flaw that may have allowed remote code execution by an attacker. A maliciously constructed project might be imported by an authorized user, resulting in remote code execution. The most recent version also included fixes for a number of additional flaws, including two distinct cross-site scripting (XSS) vulnerabilities. According to the alert, any installations running a version impacted by the problems listed below should update as soon as feasible. "When no specified deployment type of a product—such as omnibus, source code, helm chart, etc. is indicated, all types are affected."

Source	<a href="https://portswigger.net/daily-swig/gitlab-patches-critical-rce-bug-in-latest-security-release">https://portswigger.net/daily-swig/gitlab-patches-critical-rce-bug-in-latest-security-release</a>
Infected Technology	Gitlab versions 14.0 prior to 14.10.5, 15.0 prior to 15.0.4, and 15.1 prior to 15.1.1.
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-2185

---

## UnRAR path traversal flaw can lead to RCE in Zimbra

### Description

A path traversal flaw in RarLab's UnRAR binary has the potential to compromise other software and allow remote code execution (RCE) on Zimbra, a business email platform. Successful exploitation of the high severity (CVSS 7.5) issue on Zimbra, an open-source platform used by more than 200,000 businesses, "gives an attacker access to every single email sent and received on a compromised email server". They can also silently backdoor login functionalities and steal users' credentials, as well as escalate access to an organization's other internal services,

Source	<a href="https://portswigger.net/daily-swig/unrar-path-traversal-flaw-can-lead-to-rce-in-zimbra">https://portswigger.net/daily-swig/unrar-path-traversal-flaw-can-lead-to-rce-in-zimbra</a>
Infected Technology	Zimbra Business Email Platform
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-30333

---

---

## Active Exploitation of 'PwnKit' Linux Vulnerability in the Wild

### Description

The issue, tracked as CVE-2021-4034 (CVSS score: 7.8), came to light in January 2022 and concerns a case of local privilege escalation in polkit's pkexec utility, which allows an authorized user to execute commands as another user. Polkit (formerly called PolicyKit) is a toolkit for controlling system-wide privileges in Unix-like operating systems, and provides a mechanism for non-privileged processes to communicate with privileged processes. Successful exploitation of the flaw could induce pkexec to execute arbitrary code, granting an unprivileged attacker administrative right on the target machine.

Source	<a href="https://thehackernews.com/2022/06/cisa-warns-of-active-exploitation-of.html">https://thehackernews.com/2022/06/cisa-warns-of-active-exploitation-of.html</a>
--------	---

Infected Technology	Linux Operating System
---------------------	------------------------

Recommendation	Update to the latest version.
----------------	-------------------------------

CVE_ID	CVE-2021-4034
--------	---------------

---

---

## Vulnerability in Amazon Photos Android App Exposed User Information

### Description

A detail on high-severity vulnerability was published by Cybersecurity firm Checkmarx in Amazon Photos Android application that could have allowed apps to steal an Amazon access token. The issues in the application have leaked the Amazon access token, which is used for user authentication across Amazon APIs, including some personal information such as names, addresses, and emails. The issue resulted in the access token being sent in the header of the HTTP request, but the most important aspect was the fact that an attacker could control the server receiving this request.

Source	<a href="https://www.securityweek.com/vulnerability-amazon-photos-android-app-exposed-user-information">https://www.securityweek.com/vulnerability-amazon-photos-android-app-exposed-user-information</a>
--------	---

Infected Technology	Amazon Photos android app
---------------------	---------------------------

Recommendation	Update to the latest version.
----------------	-------------------------------

---

---

## Firefox 102 Patches 19 Vulnerabilities, Improves Privacy

### Description

This week, Mozilla announced the release of Firefox 102 in the stable channel, which includes fixes for 19 vulnerabilities, including four critical flaws. nsSHistory had a high-severity use-after-free flaw that may cause a crash that could be exploited while switching between XML documents. With the use of a retargeted javascript: URI, a CSP sandbox header lacking "allow-scripts" might be bypassed, a high-severity bug fixed in Firefox 102. Due to this problem, an iframe may run scripts without permission when a user clicks on a javascript: link. A flaw in Linux that makes it possible for malicious websites to make popup windows that can be enlarged in a way that the address bar is covered with online content, opening the door for spoofing attacks. We assume that several of them might have been exploited to run arbitrary code with enough effort, including ones that demonstrated JavaScript prototype or memory damage

Source	<a href="https://www.securityweek.com/firefox-102-patches-19-vulnerabilities-improves-privacy?&amp;web_view=true">https://www.securityweek.com/firefox-102-patches-19-vulnerabilities-improves-privacy?&amp;web_view=true</a>
--------	---

Infected Technology	XML documents, CSP sandbox
---------------------	----------------------------

Recommendation	Update to the latest version.
----------------	-------------------------------

CVE_ID	CVE-2022-34470, CVE-2022-34468, CVE-2022-34479, CVE-2022-34484
--------	--

---

---

## Oracle patches ‘miracle exploit’ impacting Middleware Fusion, cloud services

### Description

Oracle has patched a remote code execution (RCE) vulnerability impacting Oracle Fusion Middleware and various other Oracle systems. The "Miracle Exploit," which is a pair of serious weaknesses that can be chained together to accomplish RCE, was discovered by security researchers "Peterjson" and "Jang" and submitted to Oracle. An "easily exploitable" issue, the CVSS 9.8 bug enables unauthenticated attackers with network access to take control of an application through HTTP.

Source	<a href="https://portswigger.net/daily-swig/oracle-patches-miracle-exploit-impacting-middleware-fusion-cloud-services">https://portswigger.net/daily-swig/oracle-patches-miracle-exploit-impacting-middleware-fusion-cloud-services</a>
--------	---

Infected Technology	Fusion Middleware Various Oracle systems Oracle’s cloud infrastructure
---------------------	--

Recommendation	Update to the latest version.
----------------	-------------------------------

CVE_ID	CVE-2022-21445
--------	----------------

---

For any queries/recommendations:  
Contact us: [whois@cryptogennepal.com](mailto: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/>