

June 6,
2022

INFOSEC WEEKLY

#MADE4SECURITY

- Researchers advise to abandon Horde web client
- GitLab Issues Security Patch for Critical Account Takeover Vulnerability
- Atlassian Releases Patch for Confluence Zero-Day Flaw Exploited in the Wild
- Microsoft Releases Workarounds for Office Vulnerability Under Active Exploitation



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.

Researchers advise to abandon Horde web client

Description

The horde web client contains a critical zero-day vulnerability that can allow an attacker to compromise an organization's web server and gain foothold on the internal network. Swiss security firm Sonar (formerly SonarSource) were the ones who discovered and documented this vulnerability. The vulnerability in question abuses a GET request to perform cross-site request forgery (CSRF). An attacker can gain remote code execution (RCE) by simply sending a special crafter email. The vulnerability may never be patched as the current version of the application is flagged as the final release, so no new security updates are planned to be released.

Source	https://portswigger.net/daily-swig/horde-webmail-contains-zero-day-rce-bug-with-no-patch-on-the-horizon
--------	---

Infected Technology	Horde web client
---------------------	------------------

Recommendation	It is recommended that organizations stop the use of Horde web client and use alternatives.
----------------	---

CVE_ID	CVE-2022-30287
--------	----------------

GitLab Issues Security Patch for Critical Account Takeover Vulnerability

Description

GitLab has taken steps to resolve a significant security hole in its service that might lead to account takeover if successfully exploited. "When group SAML SSO is configured, the SCIM feature (available only on Premium+ subscriptions) may allow any owner of a Premium group to invite arbitrary users via their username and email, then change those users' email addresses via SCIM to an attacker-controlled email address and thus take over those accounts in the absence of 2FA," GitLab said.

Source	https://thehackernews.com/2022/06/gitlab-issues-security-patch-for.html
--------	---

Infected Technology	All Gitlab versions before 15.0.1
---------------------	-----------------------------------

Recommendation	Update to latest version (15.0.1)
----------------	-----------------------------------

CVE_ID	CVE-2022-1680
--------	---------------

Atlassian Releases Patch for Confluence Zero-Day Flaw Exploited in the Wild

Description

Atlassian released patches for its Confluence Server and Data Center products on Friday to address a significant security hole that has been actively exploited by threat actors to gain remote code execution. It's about a situation of Object-Graph Navigation Language (OGNL) injection on a Confluence Server or Data Center instance that might be used to execute arbitrary code. The recently disclosed flaw affects all supported versions of Confluence Server and Data Center, including all versions after 1.3.0. There are about 9,325 services running a vulnerable version of Atlassian Confluence across 8,347 separate hosts, with most instances located in the United States, China, Germany, Russia, and France.

Source	https://thehackernews.com/2022/06/atlassian-releases-patch-for-confluence.html
Infected Technology	Confluence Server or Data Center version after 1.3
Recommendation	Update to the latest version
CVE_ID	CVE-2022-26134

Microsoft Releases Workarounds for Office Vulnerability Under Active Exploitation

Description

Microsoft has issued advise for a newly found zero-day security hole in its Office productivity suite, which might be used to execute malware on vulnerable PCs. The Follina flaw, which was discovered late last week, featured a real-world exploit that used the "ms-msdt:" URI scheme to execute arbitrary PowerShell code by exploiting a flaw in a targeted Word document. An attacker who successfully exploits this flaw can execute arbitrary code with the caller application's privileges. In the context permitted by the user's permissions, the attacker can then install applications, read, alter, or remove data, and create new accounts.

Source	https://thehackernews.com/2022/05/microsoft-releases-workarounds-for.html
Infected Technology	WindowsMicrosoft Office versions Office 2013, Office 2016, Office 2019, Office 2021, Professional Plus editions
Recommendation	Open word file in Protected View or Application Guard for Office
CVE_ID	CVE-2022-30190

For any queries/recommendations:

Contact us: [whois@cryptogen**nepal**.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/>