

May 17  
2021

# INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft fixes 55 flaws including 3 zero-day vulnerabilities
- Google Patches 19 Vulnerabilities with Chrome 90 Update
- SAP Patches High-Severity Flaws in Business One, NetWeaver Products
- Cisco fixes 6-month-old AnyConnect VPN zero-day with exploit code
- Microsoft build tool used to deliver password-stealing malware
- Citrix Patches Vulnerability in Workspace App for Windows
- Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat Reader



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.

---

## 1. Microsoft fixes 55 flaws including 3 zero-day vulnerabilities

### Description

Microsoft has released May 2021 Patch Tuesday along with three-zero-day vulnerabilities within. Among the 55 patched vulnerabilities, four are classified as Critical, 50 as Important, and one as Moderate. The zero-day vulnerabilities were patched on the day after the release. Microsoft has not released the information about this attack. Among the patched vulnerabilities, three critical vulnerabilities are disclosed by Microsoft. The vulnerabilities include Privilege Escalation, Security Feature Bypass, and Remote Code Execution (RCE). The privilege escalation vulnerability resides in .NET and Visual Studio. Microsoft Exchange Server is found to be vulnerable to Security Bypass. Common utilities are identified to be vulnerable to RCE.

Source	<a href="https://msrc.microsoft.com/update-guide/vulnerability">https://msrc.microsoft.com/update-guide/vulnerability</a>
Infected Technology	Microsoft Windows and Office
CVE ID	CVE-2021-31204, CVE-2021-31207, CVE-2021-31200
Recommendation	Install Microsoft's May 2021 Patch

---

## 2. Google Patches 19 Vulnerabilities with Chrome 90 Update

### Description

The latest Chrome iteration - 90.0.4430.212 - is available for Windows, Mac, and Linux users. The Android and iOS variants of the browser were updated as well. Of the 19 security holes addressed with this release, 15 were reported by external researchers, including 13 considered high severity and two flaws rated medium severity. Chrome components affected by these issues include Web App Installs, Offline, Media Feeds, Aura, Tab Groups, Notifications, V8, Autofill, File API, History, Reader Mode, Payments, and Tab Strip. As per usual, the company isn't sharing full details on the addressed bugs until fixes have been delivered to most users. In its advisory, Google made no mention of any of these vulnerabilities being exploited in live attacks.

Source	<a href="https://chromereleases.googleblog.com/">https://chromereleases.googleblog.com/</a>
Infected Technology	Google Chrome
CVE ID	CVE-2021-30520, CVE-2021-30519, CVE-2021-30518, CVE-2021-30517, CVE-2021-30516, CVE-2021-30515, CVE-2021-30514, CVE-2021-30513, CVE-2021-30512, CVE-2021-30511, CVE-2021-30510, CVE-2021-30509, CVE-2021-30508, CVE-2021-30507, CVE-2021-30506
Recommendation	Update Google Chrome to the latest version.

---

### 3. SAP Patches High-Severity Flaws in Business One, NetWeaver Products

#### Description

SAP has released a total of six new security notes on its May 2021 Security Patch Day, along with updates for five security notes, including three related Hot News. The first updated Hot News notes deal with security updates for Chromium delivered with SAP Business Client version 90.0.4430.93, this Chromium update fixes 63 security holes. The other two updated notes patch a remote code execution vulnerability in Source Rules of SAP Commerce and a code injection issue in Business Warehouse and BW/4HANA. Three of the new security notes released on this Security Patch Day address high-severity flaws, two deal with medium-severity bugs, and one patch a low-severity issue. Of the high-severity notes, two resolves three vulnerabilities in SAP Business One. The first two flaws could lead to code injection and the third flaw could allow an attacker with access to the local SAP system to read and overwrite data or launch a denial of service (DoS) attack.

Source	<a href="https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=576094655">https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=576094655</a>
--------	---

Infected Technology	<ul style="list-style-type: none"><li>• SAP Business Client version 6.5</li><li>• SAP Commerce versions – 1808, 1811, 1905, 2005, 2011</li><li>• SAP Business Warehouse versions – 700, 701, 702, 711, 730, 731, 740, 750, 782</li><li>• SAP BW4HANA versions – 100, 200</li><li>• NetWeaver AS ABAP versions – 700, 701, 702, 730, 731</li></ul>
---------------------	---

CVE ID	CVE-2021-27602, CVE-2021-21466, CVE-2021-27611
--------	--

Recommendation	Consider applying the security patches.
----------------	---

---

#### 4. Cisco fixes 6-month-old AnyConnect VPN zero-day with exploit code

##### Description

Cisco has fixed a six-month-old zero-day vulnerability found in the Cisco AnyConnect Secure Mobility Client VPN software, with publicly available proof-of-concept exploit code. Cisco disclosed this bug in November 2020 without releasing security updates but provided mitigation measures to decrease the attack surface. While the Cisco Product Security Incident Response Team (PSIRT) said that CVE-2020-355 proof-of-concept exploit code is available, it also added that there is no evidence of attackers exploiting it in the wild. The vulnerability is now addressed in Cisco AnyConnect Secure Mobility Client Software releases 4.10.00093 and later. These new versions also introduce new settings to help individually allow/disallow scripts, help, resources, or localization updates in the local policy, settings that are strongly recommended for increased protection.

Source	<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK</a>
--------	---

Infected Technology	Cisco AnyConnect Secure Mobility Client VPN software
---------------------	--

CVE ID	CVE-2020-3556
--------	---------------

Recommendation	Consider installing the security updates provided by cisco.
----------------	---

---

---

## 5. Microsoft build tool used to deliver password-stealing malware

### Description

Malicious actors have exploited Microsoft Build Engine (MSBuild) to deploy remote access tools (RAT). The actors installed an information-stealing malware fileslessly as a part of their ongoing campaign. MSBuild (msbuild.exe) is an open-source Microsoft development platform to build the application. Anomali's Threat Research team observed that the malicious MSBuild project file delivered were bundled with encoded shellcodes and executables. The threat actors have used these as a tool for injecting final payloads into the memory of the processes. The attackers focused on pushing Quasar RAT, Remcos RAT, and Stealer payload malware in the victim's computer to harvest keystrokes, credentials, snapshot, gain persistence, disable anti-malware and take control of the device completely.

Source	<a href="https://www.anomali.com/blog/threat-actors-use-msbuild-to-deliver-rats-filelessly">https://www.anomali.com/blog/threat-actors-use-msbuild-to-deliver-rats-filelessly</a>
--------	---

Infected Technology	Microsoft MSBuild (msbuild.exe)
---------------------	---------------------------------

---

---

## 6. Citrix Patches Vulnerability in Workspace App for Windows

### Description

Citrix this week announced that it has patched a local privilege escalation vulnerability in the Citrix Workspace app for Windows. The vulnerability could be exploited by local attackers to escalate their privileges to the SYSTEM level. All supported versions of the Citrix Workspace app for Windows are affected by the security hole. The issue, however, only impacts those Windows systems on which the Workspace application was installed using an account with administrator privileges (either local or domain admin). Systems on which a standard Windows user account was used to install the Citrix Workspace app are not affected. The tech giant advises customers to update their applications to a patched version as soon as possible, to ensure they are safe from potential exploitation attempts. Those who have automatic updates enabled will automatically receive the security update.

Source	<a href="https://support.citrix.com/article/CTX307794">https://support.citrix.com/article/CTX307794</a>
--------	---

Infected Technology	Citrix Workspace App 2105 and later Citrix Workspace App 1902 LTSR CU4 and later
---------------------	---

CVE ID	CVE-2021-22907
--------	----------------

Recommendation	Consider updating Citrix Workspace to the patched version.
----------------	--

---

---

## 7. Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat Reader

### Description

Adobe is warning its customers of a critical zero-day bug actively exploited in the wild that affects its ubiquitous Adobe Acrobat PDF reader software. A patch is available that consists of 43 fixes for 12 of its products, including Adobe Creative Cloud Desktop Application, Illustrator, InDesign, and Magento. In all, Adobe Acrobat received 10 critical and four important vulnerability patches. Seven out of those bugs included arbitrary code execution bugs. Three of the vulnerabilities patched this Tuesday open system up to out-of-bounds write attacks. Adobe Illustrator received the next highest number of patches on Tuesday, with five critical code execution vulnerabilities fixed. According to Adobe's description of the flaws, three are memory corruption bugs that open systems up to hackers, triggering arbitrary code execution on targeted systems.

Source	<a href="https://helpx.adobe.com/security/products/acrobat/apsb21-29.html">https://helpx.adobe.com/security/products/acrobat/apsb21-29.html</a>
--------	---

Infected Technology	<ul style="list-style-type: none"><li>• Windows Acrobat DC &amp; Reader DC (versions 2021.001.20250 and earlier)</li><li>• MacOS Acrobat DC &amp; Reader DC (versions 2021.001.20149 and earlier)</li><li>• Windows and macOS Acrobat 2020 &amp; Acrobat Reader 2020 (2020.001.30020 and earlier versions)</li><li>• Windows &amp; macOS Acrobat 2017 &amp; Acrobat Reader 2017 (2017.011.30194 and earlier)</li></ul>
---------------------	--

CVE ID	CVE-2021-28500, CVE-2021-21044, CVE-2021-21038, CVE-2021-21086, CVE-2021-21103, CVE-2021-21104, CVE-2021-21105
--------	--

Recommendation	Consider updating the product installations to the latest patched versions.
----------------	---

---

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/>