

# OWASP Top 10 - A06:2021 Vulnerable and Outdated Components

Presented By- Sanchay & Jalaj  
null-meet Delhi @  
Airtel Centre, Gurugram  
25 February 2023



**Sanchay@null:~\$ whoami**

- With over 4-5 years of Practical experience in the field, I have good knowledge of Bug Hunting and PenTesting, especially System Hacking.
- Co-Founder of HackersVilla CyberSecurity Pvt Ltd, a security community and B2B VAPT Services Platform.

-----

- Email : sanchayofficial
- Instagram : @sanchayofficial
- LinkedIn : sanchayofficial



■ Jalaj@null:~\$ whoami

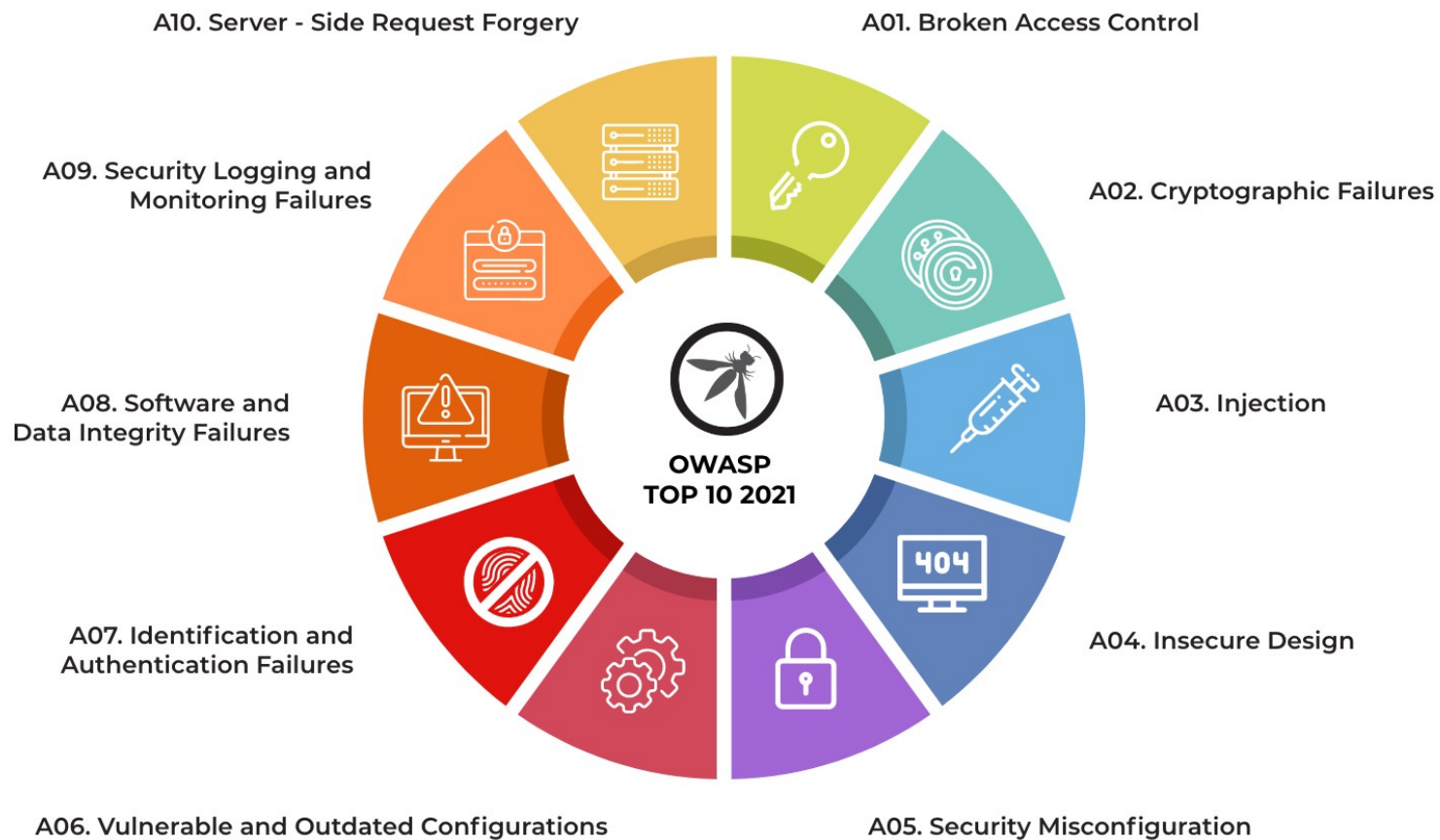
- Cyber Security Geek
- CTF Player
- Security Analyst
- Wears the Blue cape
- Threat Hunting



# Structure of Presentation



1. Introduction
2. What are Vulnerable and Outdated Components?
3. Why are Vulnerable and Outdated Components a Problem?
4. How to Identify and Mitigate Vulnerable and Outdated Components
5. Case Studies and Examples
6. Conclusion



## A06:2021 – Vulnerable and Outdated Components



It was #2 from the Top 10 community survey but also had enough data to make the Top 10 via data. Vulnerable Components are a known issue that we struggle to test and assess risk and is the only category to not have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploits/impact weight of 5.0 is used. Notable CWEs included are CWE-1104: Use of Unmaintained Third-Party Components and the two CWEs from Top 10 2013 and 2017.



# Mapped Common Weakness Enumeration (CWE's)

---

- CWE-937 OWASP Top 10 2013: Using Components with Known Vulnerabilities
- CWE-1035 2017 Top 10 A9: Using Components with Known Vulnerabilities
- CWE-1104 Use of Unmaintained Third Party Components

# What Components are we talking about in A06 ?

- Libraries, Ex- JQuery, AngularJS, Bootstraao, etc.
- Frameworks, Ex- Django, Flask, Ruby on Rails, etc.
- Modules, Ex – SSL, pip, urllib, etc.



# What makes a component vulnerable or outdated ?

chromium / chromium Public

Notifications Fork 5.3k Star 14.1k

<> Code Pull requests 60 Actions Security Insights

main 8 branches 26,156 tags Go to file Code

| chromium-autoroll and Chromium LUCI CQ Roll Depot Tools from 2... f306f50 8 minutes ago 1,231,020 commits |   |                |
|---|---|----------------|
| android_webview   | Reland "[Autofill] Move ownership of ContentAutofillDriverFactory ... | 39 minutes ago |
| apps  | Enable -Wexit-time-destructors for //apps/ui/views.                   | last week      |
| ash   | Switch to simpler base::WriteFile() variants (48/N)                   | 13 minutes ago |
| base  | Add trace event counters for LCDText                                  | 1 hour ago     |
| build   | Report WebView multiprocess mode in variant instead of test name ...  | 1 hour ago     |
| build_overrides   | Allow projects embedding Chrome to disable libc++ hardening.          | last week      |
| buildtools  | Roll libc++ from 09f68a400f92 to e136ec5032a5 (3 revisions)           | yesterday      |
| cc  | Add trace event counters for LCDText                                  | 1 hour ago     |
| chrome  | [CodeHealth] Converting QuotaErrorOr to base::expected                | 18 minutes ago |
| chromecast  | Switch to simpler base::WriteFile() variants (61/N)                   | 25 minutes ago |
| chromeos  | [PhoneHub] Fix duplicate old notification                             | 48 minutes ago |
| codelabs  | SequenceManager: Make priorities configurable (yield API 1/n)         | last week      |

About

The official GitHub mirror of the Chromium source

[chromium.googlesource.com/chromi...](https://chromium.googlesource.com/chromi...)

Readme

BSD-3-Clause, BSD-3-Clause licenses found

Code of conduct

14.1k stars

528 watching

5.3k forks

Releases

26,156 tags

Packages


No packages published

# Why vulnerable components a problem ?

**F** [https://www.forbes.com › sites › gordonkelly › 2022 › 08 › 31 › google-chrome-105-new-vulnera...](https://www.forbes.com/sites/gordonkelly/2022/08/31/google-chrome-105-new-vulnera...)

## Google Chrome 105 Released To Patch 24 New Vulnerabilities

31 Aug 2022 · Multiple new high-level threats have been found in Google Chrome. LIGHTROCKET VIA GETTY IMAGES. This is a list of the nine most serious new Chrome vulnerabilities: Critical - CVE-2022-3038: Use ...

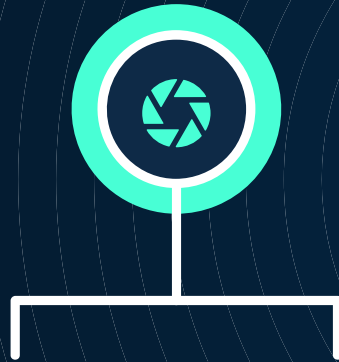
 [https://www.tomsguide.com › news › chrome-91-update-2](https://www.tomsguide.com/news/chrome-91-update-2)

## Google Chrome zero-day flaw under attack — what to do now

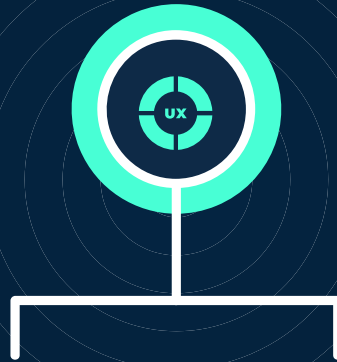
10 Jun 2021 · Chrome in-the-wild vulnerability CVE-2021-30551 patched today was also from the same actor and targeting. Thanks to ... Here's a list of the most recent Chrome/Chromium updates. June 9: 91.0.4472 ...

# Why vulnerable components a problem ?

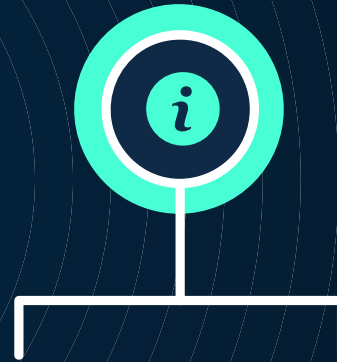
---



**Shellshock**



**F5 BIG-IP**



**Log4j**

# How to Identify and Mitigate Vulnerable and Outdated Components

---

1. Remove unused dependencies, unnecessary features, components, files, and documentation.
2. Continuously inventory the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies using tools like versions, OWASP Dependency
3. Subscribe to email alerts for security vulnerabilities related to components you use.
4. Only obtain components from official sources over secure links.
5. Monitor for libraries and components that are unmaintained or do not create security patches for older versions.

Thank you,



Any questions ?

