Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the internet. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE

Google is aware that an exploit for vulnerability CVE-2023-5217 exists in the wild.

SYSTEMS AFFECTED:

- Chrome versions prior to 117.0.5938.132 for Windows, Mac and Linux

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001)

Technique: *Drive-By Compromise* (T1189)

- Heap buffer overflow in vp8 encoding in libvpx. (CVE-2023-5217)
- Use after free in Extensions. (CVE-2023-51872)
- Use after free Passwords. (CVE-2023-5186)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS

We recommend the following actions be taken:

- Apply appropriate updates provided by Google to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)

- **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
  - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
  - **Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients:** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)

  - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
  - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048: Application Isolation and Sandboxing**)

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)

  - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)

  - **Safeguard 9.2: Use DNS Filtering Services:** Use DNS filtering services on all enterprise assets to block access to known malicious domains.
  - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
  - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise's email gateway.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. (**M1017: User Training**)

- **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
- **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

REFERENCES

Google:
https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_27.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5186
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5187
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5217