

Overall rating: High



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple vulnerabilities recently disclosed in Microsoft Edge Chromium below 114.0.1823.67.

Technical Details

- **Remote Type Confusion Vulnerability in V8** - CVE-2023-3420
Type Confusion in V8 in Microsoft Edge Chromium prior to 114.0.1823.67 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
- **Remote Use After Free Vulnerability in Media** - CVE-2023-3421
Use after free in Media in Microsoft Edge Chromium prior to 114.0.1823.67 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
- **Remote Use After Free Vulnerability in Guest View** - CVE-2023-3422
Use after free in Guest View in Microsoft Edge Chromium prior to 114.0.1823.67 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.

These vulnerabilities are rated as a **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify [VRM](#) with any questions or concerns you may have.

References

- CVE-2023-3420, CVE-2023-3421, CVE-2023-3422
- <https://msrc.microsoft.com/update-guide/>
- <https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-3420>
- <https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-3421>
- <https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2023-3422>