



CVE-2023-36787

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-36787 |
| State | PUBLIC |
| Assigner | secure@microsoft.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-08-21 20:15:00 UTC |
| Updated | 2024-02-03 09:15:00 UTC |
| Description | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability |

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------------|-------------------------------|---------|--------|---------|----------|
| Application | Microsoft | Edge Chromium | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|---|---------------------|
| Security Update Guide - Microsoft Security Response Center | MISC | msrc.microsoft.com | |
| Microsoft Edge: Multiple Vulnerabilities (GLSA 202402-05) — Gentoo security | | security.gentoo.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378795](#) Microsoft Edge Based on Chromium Prior to 116.0.1938.54 Multiple Vulnerabilities

[710855](#) Gentoo Linux Microsoft Edge Multiple Vulnerabilities (GLSA 202402-05)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)