Severity

High

Analysis Summary

CVE-2022-1477, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Vulkan. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1478, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in SwiftShader. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1479, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in ANGLE. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1480, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Device API. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1481, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Sharing. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1482, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by inappropriate implementation in WebGL. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1483, CVSS 8.8

Google Chrome is vulnerable to a heap-based buffer overflow, caused by improper bounds checking by WebGPU. By persuading a victim to visit a specially crafted Web site, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the application to crash.

CVE-2022-1484, CVSS 8.8

Google Chrome is vulnerable to a heap-based buffer overflow, caused by improper bounds checking by Web UI Settings. By persuading a victim to visit a specially crafted Web site, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the application to crash.

CVE-2022-1486, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a type confusion inV8. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1487, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Ozone. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1488, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by inappropriate implementation in Extensions API. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1489, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds memory access in UI Shelf. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1490, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Browser Switcher. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1491, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Bookmarks. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1492, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by insufficient data validation in Blink Editing. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1493, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Dev Tools. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1494, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by insufficient data validation in Trusted Types. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1495, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by incorrect security UI in Downloads. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1496, CVSS 8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in File Manager. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1497, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by inappropriate implementation in input. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1498, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by inappropriate implementation in HTML Parser. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1499, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by inappropriate implementation in WebAuthentication. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1500, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by insufficient data validation in Dev Tools. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1501, CVSS 6.5

Google Chrome could allow a remote attacker to bypass security restrictions, caused by inappropriate implementation in iframe. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

Impact

- Bypass Security
- Gain Access

Indicators Of Compromise

CVE

- CVE-2022-1477
- CVE-2022-1478
- CVE-2022-1479
- CVE-2022-1480
- CVE-2022-1481
- CVE-2022-1482
- CVE-2022-1483
- CVE-2022-1484
- CVE-2022-1486
- CVE-2022-1487
- CVE-2022-1488
- CVE-2022-1489
- CVE-2022-1490
- CVE-2022-1491
- CVE-2022-1492
- CVE-2022-1493
- CVE-2022-1494
- CVE-2022-1495
- CVE-2022-1496
- CVE-2022-1497
- CVE-2022-1498

- CVE-2022-1499
- CVE-2022-1500
- CVE-2022-1501

Affected Vendors

- Google

Affected Products

- Google Chrome 101.0

Remediation

Upgrade to the latest version of Chrome, available from the Google Chrome Releases Web site.

Google Chrome Releases Web Site