Severity

High

Analysis Summary

CVE-2022-1305 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in storage. 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-2022-1306 CVSS:6.5

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by inappropriate implementation in compositing. 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-2022-1307 CVSS:6.5

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by inappropriate implementation in full screen. 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-2022-1308 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in BFCache. 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-2022-1309 CVSS:6.5

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by insufficient policy enforcement in developer 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-2022-1310 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in regular expressions. 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-2022-1311 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Chrome OS shell. 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-2022-1312 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in storage. 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-2022-1313 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in tab groups. 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-2022-1314 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a type confusion in V8. 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.

Impact

- Code Execution
- Security Bypass
- Denial of Service

Indicator Of Compromise

CVE

- CVE-2022-1305
- CVE-2022-1306
- CVE-2022-1307
- CVE-2022-1308
- CVE-2022-1309
- CVE-2022-1310
- CVE-2022-1311
- CVE-2022-1312
- CVE-2022-1313
- CVE-2022-1314Google Chrome 100[.]0

Affected Vendors

Google

Affected Products

- Google Chrome 100.0

Remediation

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

Google Chrome Releases Website