Severity

High

Analysis Summary

CVE-2022-1641 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Web UI Diagnostics. 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-2022-1640 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-2022-1639 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-2022-1638 CVSS:8.8

Google Chrome is vulnerable to a heap-based buffer overflow, caused by improper bounds checking in V8 Internationalization. By persuading a victim to visit a specially crafted Web site, a remote attacker could overflow a buffer and execute arbitrary code or cause a denial of service condition on the system.

CVE-2022-1637 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by an inappropriate implementation in Web Contents. 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-2022-1636 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Performance APIs. 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-2022-1635 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Permission Prompts. 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-2022-1634 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 UI. 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-2022-1633 CVSS:8.8

Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Sharesheet. 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
- Buffer Overflow

Indicators Of Compromise

CVE

- CVE-2022-1641
- CVE-2022-1640
- CVE-2022-1639
- CVE-2022-1637
- CVE-2022-1636
- CVE-2022-1635
- CVE-2022-1634

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