Severity

High

Analysis Summary

CVE-2022-1855 CVSS:8.8 Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Messaging. 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-2022-1854 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-2022-1854 CVSS:8.8 Google Chrome could allow a remote attacker to bypass security restrictions, caused by improper policy enforcement in File System API. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1876 CVSS:5.4 Google Chrome is vulnerable to a heap-based buffer overflow, caused by improper bounds checking in DevTools. By persuading a victim to visit a specially crafted Web site, a remote attacker could overflow a buffer and execute arbitrary code cause a denial of service condition on the system.

CVE-2022-1875 CVSS:4.3 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper implementation in PDF. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1874 CVSS:4.3 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper policy enforcement in Safe Browsing. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1873 CVSS:4.3 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper policy enforcement in COOP. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1872 CVSS:4.3 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper policy enforcement in Extensions API. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1871 CVSS:4.3 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper policy enforcement in File System API. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1870 CVSS:8.8 Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in App Service. 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-2022-1869 CVSS:6.5 Google Chrome could allow a remote attacker to obtain sensitive information, caused by a type confusion in V8. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1868 CVSS:6.5 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper implementation in Extensions API. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1867 CVSS:6.5 Google Chrome could allow a remote attacker to obtain sensitive information, caused by improper validation of untrusted input in Data Transfer. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1866 CVSS:8.8 Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Tablet Mode. 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-2022-1865 CVSS:8.8 Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in WebApp Installs. 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-2022-1864 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-2022-1863 CVSS:6.5 Google Chrome could allow a remote attacker to obtain sensitive information, caused by an improper implementation in Extensions. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1862 CVSS:6.5 Google Chrome could allow a remote attacker to obtain sensitive information, caused by an improper implementation in Extensions. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1861 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-2022-1860 CVSS:8.8 Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in UI Foundations. 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-2022-1859 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 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-2022-1858 CVSS:.6.5 Google Chrome could allow a remote attacker to obtain sensitive information, caused by an out-of-bounds read in DevTools. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1858 CVSS:8.8 Google Chrome could allow a remote attacker to bypass security restrictions, caused by improper policy enforcement in File System API. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to bypass security restrictions.

CVE-2022-1856 CVSS:8.8 Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in User Education. 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 Buffer Overflow Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-1855
- CVE-2022-1854
- CVE-2022-1854
- CVE-2022-1876
- CVE-2022-1875
- CVE-2022-1874

- CVE-2022-1873
- CVE-2022-1872
- CVE-2022-1871
- CVE-2022-1870
- CVE-2022-1869
- CVE-2022-1868
- CVE-2022-1867
- CVE-2022-1866
- CVE-2022-1865
- CVE-2022-1864
- CVE-2022-1863
- CVE-2022-1862
- CVE-2022-1861
- CVE-2022-1860
- CVE-2022-1859
- CVE-2022-1858
- CVE-2022-1858

Affected Vendors

- Google

Affected Products

- Google Chrome 102.0

Remediation

Upgrade to the latest version of Chrome (102.0.5005.61 or later), available from the Google Chrome Releases Website.

Google Chrome Releases Website