Previous article Next article

Google to Pay For Bugs Found in Chromium

Author:
Dennis Fisher

January 29, 2010 / 11:31 am

Google is starting a new program that will pay security researchers a $500 bounty for every security bug they find in Chromium, the open-source codebase behind the Google Chrome browser, as well as for bugs found in Chrome itself.

Google is starting a new program that will pay security researchers a $500 bounty for every security bug they find in Chromium, the open-source codebase behind the Google Chrome browser, as well as for bugs found in Chrome itself.

The company said Thursday that the plan is both meant as a reward for researchers who have been contributing bugs to the project already, and as a way to encourage other researchers to find security flaws in Chromium. Google said it will pay a base bounty of $500 for most bugs contributed, but may raise the payment to $1337 for bugs that are "particularly severe or particularly clever." The program is modeled after one started some time ago by Mozilla, which also pays $500 bounties.

be

In addition to paying for bugs in Chromium and Chrome, Google said it may buy bugs discovered in plug-ins and components.

"In addition, bugs in plugins that are part of the Chromium project and shipped with Google Chrome by default (e.g. Google Gears) may be eligible. Bugs in third-party plugins and extensions are ineligible," the company said.

Other organizations have been buying vulnerabilities privately for several years now, most notably the Zero Day Initiative from Tipping Point, and VeriSign's iDefense Labs unit. Those companies pay far more than $500 for vulnerabilities, and researchers say that private organizations, such as government agencies, routinely pay tens of thousands of dollars for critical remotely exploitable bugs in popular software.

Web Security

SUGGESTED ARTICLES

Google Patches Chrome's Fifth Zero-Day of the Year

An insufficient validation input flaw, one of 11 patched in an update this week, could allow for arbitrary code execution and is under active attack.

August 18, 2022

Google Warns of Critical Android Remote Code Execution Bug

Google's Android security update addressed 43 bugs overall affecting Android handsets, including Samsung phones.

January 5, 2021 2

Researcher Bre reCAPTCHA Wi Speech-to-Text

Researcher uses an trick against latest th reCAPTCHA, with a rate.

January 4, 2021

INFOSEC INSIDER

Why Physical Security Maintenance Should Never Be an Afterthought

July 25, 2022

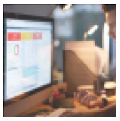
Conti's Reign of Chaos: Costa Rica in the Crosshairs

July 20, 2022

How War Impacts Cyber Insurance

July 12, 2022

Rethinking Vulnerability Management in a Heightened Threat Landscape



July 11, 2022

Twitter

Tens of thousands of cameras have failed to patch a critical, 11-month-old CVE, leaving thousands of organizations... https://t.co/iYq3WeTkbf

4 months ago

Follow @threatpost

The First Stop For Security News

Privacy Policy

Terms and Conditions