kindred

Security Newsletter

11 March 2019

Subscribe to this newsletter

Serious Chrome zero-day exploited in the wild, update "right this minute"

You must update your Google Chrome immediately to the latest version of the web browsing application.

Security researcher Clement Lecigne of Google's Threat Analysis Group discovered and reported a high severity vulnerability in Chrome late last month that could allow remote attackers to execute arbitrary code and take full control of the computers. The vulnerability, assigned as CVE-2019-5786, affects the web browsing software for all major operating systems including Microsoft Windows, Apple macOS, and Linux.

What's more worrisome? Google warned that this zero-day RCE vulnerability is actively being exploited in the wild by attackers to target Chrome users. It appears to exploit this vulnerability, all an attacker needs to do is tricking victims into just opening, or redirecting them to, a specially-crafted webpage without requiring any further interaction.

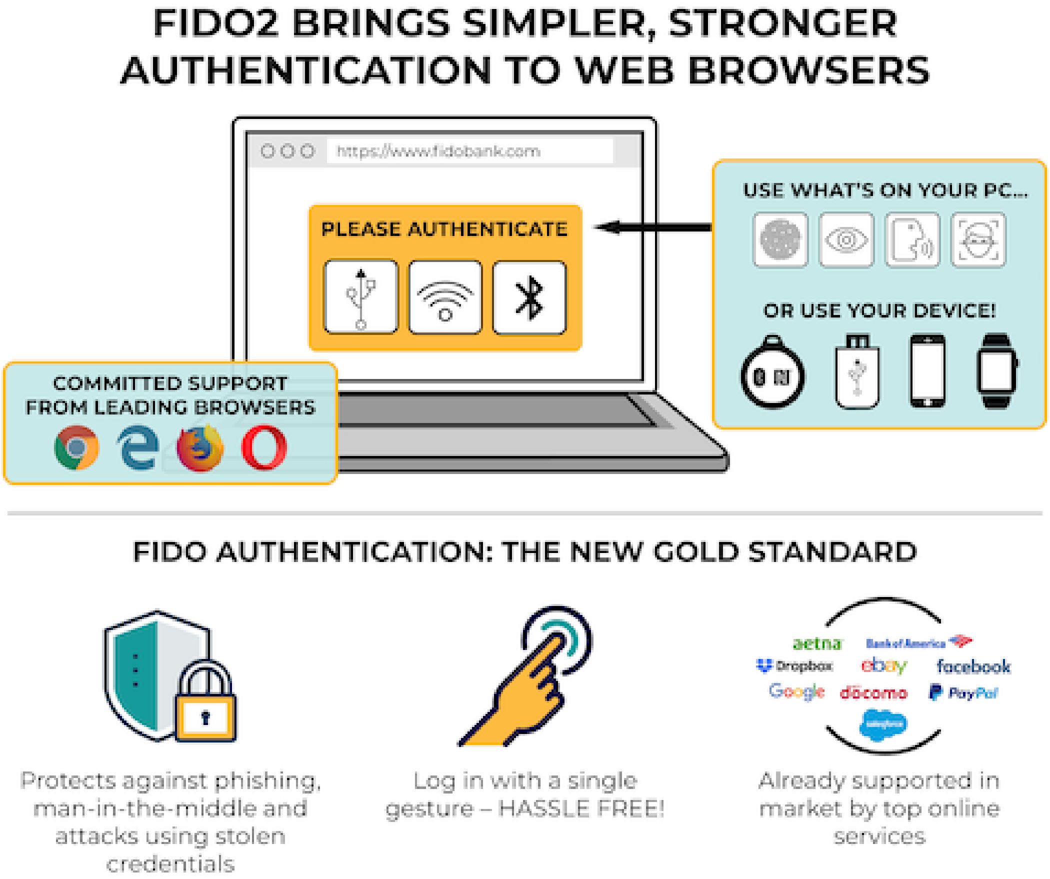
To check that you're up-to-date, go to the About Google Chrome… window, accessible from the address bar by typing in the special URL chrome://settings/help. This will not only show the current version but also do an update check at the same time, just in case any recent auto-updates have failed or your computer hasn't called home yet.

Read More on NakedSecurity

Even More on TheHackerNews

Official Google Statement

W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins


FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS
https://www.fidobank.com
PLEASE AUTHENTICATE
USE WHAT'S ON YOUR PC...
OR USE YOUR DEVICE!
COMMITTED SUPPORT FROM LEADING BROWSERS
FIDO AUTHENTICATION: THE NEW GOLD STANDARD
aetna
Bank of America
Dropbox
ebay
facebook
Google
docomo
PayPal
salesforce
Protects against phishing, man-in-the-middle and attacks using stolen credentials
Log in with a single gesture – HASSLE FREE!
Already supported in market by top online services

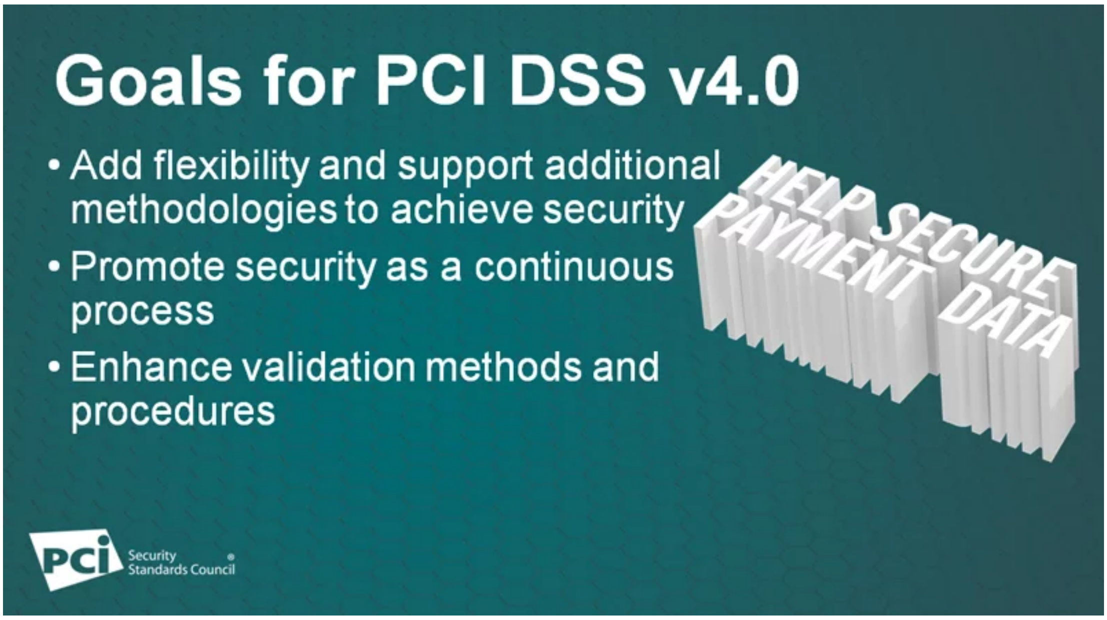
Major browsers and platforms have built-in support for new web standard for easy and secure logins via biometrics, mobile devices and FIDO security keys.

The World Wide Web Consortium (W3C) and the FIDO Alliance today announced the Web Authentication (WebAuthn) specification is now an official web standard. This advancement is a major step forward in making the web more secure – and usable – for users around the world.

WebAuthn allows users to log into their internet accounts using their preferred device. Web services and apps can – and should – turn on this functionality to give their users the option to log in more easily via biometrics, mobile devices and/or FIDO security keys, and with much higher security over passwords alone.

Read More on FidoAlliance

PCI DSS: Looking Ahead to Version 4.0



Goals for PCI DSS v4.0

- Add flexibility and support additional methodologies to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures

HELP SECURE PAYMENT DATA
PCI Security Standards Council

PCI SSC has begun efforts on PCI Data Security Standard version 4.0 (PCI DSS v4.0). PCI DSS v4.0 will incorporate input received from global PCI SSC stakeholders during the 2017 request for comments (RFC) period.

Some of the specific areas that stakeholders asked PCI SSC to review include: Authentication, specifically consideration for the NIST MFA/password guidance; Broader applicability for encrypting cardholder data on trusted networks; Monitoring requirements to consider technology advancement and Greater frequency of testing of critical controls.

PCI DSS v4.0 is not anticipated for release prior to late 2020. Specific timing on the release is dependent upon feedback received during the development period.

Read More on PCI Blog

More #News

- Slack, GitHub Abused by New SLUB Backdoor in Targeted Attacks
- Using your Office 365 Secure Score
- 12,449 Data Breaches Confirmed in 2018, a 424% Increase Over the Previous Year
- Notepad++ No Longer Code Signed, Dev Won't Support Overpriced Cert Industry
- Singapore proposes new security guidelines to beef up financial resilience
- #Opfail: Phisher Attaches Powershell Exec Instead of Malware
- Google reveals BuggyCow macOS security flaw
- Google Launches Backstory — A New Cyber Security Tool for Businesses
- Unpatched UPnP-Enabled Devices Left Exposed to Attacks
- Saudi caller ID app leaves data of 5+ million users in unsecured MongoDB server
- What is Mimikatz? And how to defend against this password stealing tool
- Comcast security nightmare: default '0000' PIN on everybody's account
- Open source software breaches surge in the past 12 months
- Security Alert: Malware Hides in Script Injection, Bypassing AV Detection
- Citrix Learns About Internal Network Security Breach from FBI
- Cybersecurity Firm Finds Increasingly Complex and Common Malware Inside of Ad Networks

#Patch Time!

- Cisco tells Nexus switch owners to disable POAP feature for security reasons
- Update now! Critical Adobe ColdFusion flaw now being exploited
- Windows 10 IoT Core Test Interface Lets Attackers Take Over Devices
- Google: Chrome zero-day was used together with a Windows 7 zero-day

#Tech and #Tools

- Ghidra: Software reverse engineering (SRE) framework developed by NSA's Research Directorate
- The Hitchhiker's Guide To Initial Access
- SirepRAT: Remote Command Execution as SYSTEM on Windows IoT Core
- "Can I take over XYZ?" — how to claim (sub)domains with dangling DNS records.
- Gone in six seconds? Exploiting car alarms
- Top 5 Ways The Red Team breached and assessed the Physical Environment
- Penetration Testing Active Directory, Part I
- Windows 7 may insecurely load Dynamic Link Libraries
- MouseJack: From Mouse to Shell – Part 1
- Windows Exploit Suggester - Next Generation

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us