Chapter 38 of the Society of Broadcast Engineers

SBE

EL PASO - LAS CRUCES - JUAREZ

FEBRUARY 2023

PO Box 3561 El Paso, TX 79923-3561 www.kint98.com

NEWS

SECURITY PATCHES

You Really Need to Update Firefox and Android Right Now

January saw a slew of security patches for iOS, Chrome, Windows, and more.

THE NEW YEAR has kicked off with some hefty security updates released by the likes of Apple, Google, and Microsoft. January has been a busy time for enterprise patches too, with SAP, VMWare, and Oracle among those issuing security fixes during the month.

Here’s everything you need to know about the security fixes released in January.

Apple iOS

Apple has released iOS 16.3 along with a new feature that allows you to use security keys as an extra layer of protection for your Apple ID. Apple’s latest update also comes with 13 security fixes, including three in WebKit, the engine that powers the Safari browser, two of which could allow code execution.

Another three issues have been patched in the iPhone Kernel at the heart of iOS. One of the vulnerabilities, tracked as CVE-2023-23504, is pretty serious—if exploited, it could result in an app being able to execute code with Kernel privileges.

Apple also released iOS 15.7.3 for users of older iPhones, fixing six security issues including the Kernel code execution bug patched in iOS 16.3. None of the issues fixed in iOS 15.7.3 or iOS 16.3 are believed to have been used in real-life attacks. However, Apple has released iOS 12.5.7 for older devices to patch an already exploited WebKit vulnerability, CVE-2022-42856. The iPhone maker fixed the same bug for smartphones using iOS 15 in December.

Apple’s January updates also include tvOS 16.3, Safari 16.3, macOS Big Sur 11.7.3, macOS Monterey 12.6.3, watchOS 9.3, and macOS Ventura 13.2.

Google Chrome

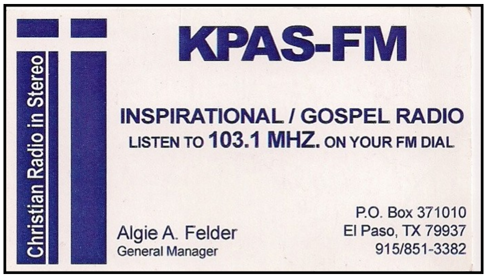
It was a busy start to the year for Google, which has fixed 17 vulnerabilities in its Chrome browser, two of which are rated as having a high impact. The first of the two issues, tracked as CVE-2023-0128, is a use-after-free bug in Overview Mode. Meanwhile, CVE-2023-0129 is a heap buffer overflow issue in Network Service. Eight of the patched vulnerabilities are marked as having a medium impact, including CVE-2023-0130, an inappropriate implementation bug in Fullscreen, and CVE-2023-0137, a heap buffer overflow issue in Platform Apps.

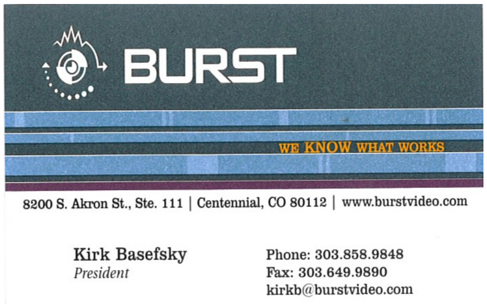
Later in the month, Google patched six Chrome issues, including two rated as having a high impact. CVE-2023-0471 is a use-after-free bug in WebTransport and CVE-2023-0472 is a use-after-free bug in WebRTC. The first Chrome patches of 2023 do not include any already exploited issues, so although the update is important, it’s not as urgent as some of Google’s recent version releases. Last year, the browser maker patched nine zero day vulnerabilities

Google Android

Google has posted its Android Security Bulletin including a number of patches for Android devices. The most severe flaw is a security vulnerability in the Framework component that could lead to local escalation of privilege with no additional privileges needed. CVE-2022-20456 is rated as having a high severity and affects Android versions 10 through 14. Meanwhile, CVE-2022-20490 is another local escalation of privilege bug that does not require user interaction to be exploited.

Google also fixed vulnerabilities in the Kernel, including three remote code execution (RCE flaws marked as critical. CVE-2022-42719 is a use-after-free bug that could be used by attackers to crash the Kernel and execute code. Google has fixed several issues in the System, the most severe of which could lead to local escalation of privilege.





The Android security patch is available to Google's Pixel devices, which have their own specific updates, and Samsung's Galaxy range, including Samsung Galaxy Note 10, Galaxy S21, and Galaxy A73. You can check for the update in your settings

Microsoft Patch Tuesday

Microsoft fixed a rather hefty 98 security issues in its first Patch Tuesday of the year, including an already exploited vulnerability: CVE-2023-21674 is an elevation of privilege flaw impacting the Windows Advanced Local Procedure Call that could lead to browser sandbox escape.

By exploiting the bug, an adversary could gain System privileges, Microsoft wrote, confirming that the flaw has been detected in real-life attacks.

Another elevation of privilege vulnerability in the Windows Credential Manager User Interface, CVE-2023-21726, is relatively easy to exploit and doesn't require any interaction from the user.

January's Patch Tuesday also saw Microsoft fix nine Windows Kernel vulnerabilities, eight of which are elevation of privilege issues and one information disclosure vulnerability.

Mozilla Firefox

Software firm Mozilla has released important updates for its Firefox browser, the most serious of which have been the subject of a warning by the US Cybersecurity and Infrastructure Security Agency (CISA).

Among the 11 flaws fixed in Firefox 109 are four rated as having a high impact, including CVE-2023-23597, a logic bug in process allocation that could allow adversaries to read arbitrary files.

Meanwhile, Mozilla said its security team found memory safety bugs in Firefox 108. "Some of these bugs showed evidence of memory corruption and we presume that with enough effort, some could have been exploited to run arbitrary code," it wrote.

An attacker could exploit some of these vulnerabilities to take control of an affected system, CISA said in its advisory. "CISA encourages users and administrators to review Mozilla's security advisories for Firefox ESR 102.7 and Firefox 109 for more information and apply the necessary updates."

continue in page 5

SBE CHAPTER 38 OFFICERS

CHAIRMAN
Antonio Castro
SBE member # 11456.
KFOX/COX retired Chief Eng.
800 Arredondo dr.
El Paso. TX 79912
915-584-1220 home
915-525-8507 cell
farahjac@sbcglobal.net

VICE CHAIRMAN
Bruno Cruz
SBE member # 25867
200 E.Alto Mesa
El Paso, TX.79912
915-757-7898
915-526-1842 cell
Bruno.cruzJR@kfoxtv.com

TREASURER
Walter Hanthorn
SBE member # 18307
KSCE TV
4461 Gen. Maloney
El Paso, TX. 79924
915-269-7583 home
915-532-8588 office

CERTIFICATION COMMITTEE:
David Halperin.

MEMBERSHIP COMMITTEE:
Antonio Castro
Warren Reeves

FREQUENCY COORDITATION COMMITTEE:
Warren Reeves
Owen Smith

SCHOLARSHIP COMMITTEE:
Rick Vilardell

WEB SITE COMMITTEE:
Norbert Miles

SUSTAINING MEMBERSHIP:
Antonio Castro

PROGRAM CHAIRMAN:
Warren Reeves

NEWSLETTER:
Antonio Castro

EAS CHAIRMAN:
Michael Rivera

EXECUTIVE COMMITTEE:
Antonio Castro
Bruno Cruz
Walter Hanthorn

EL PASO, TX SBE CHAPTER 38 MEETING MINUTE

DATE 1 /10/2023 LOCATION: LUBY'S CAFETERIA

MEETING CALLED TO ORDER: 12:32 PM , BY ANTONIO CASTRO. WE WERE 7(SEVEN) ATTENDANTS

REPORT OF THE SECRETARY: MINUTES IN THE JANUARY NEWSLETTER. ACCEPTED BY NORBERT MILES, SECONDED BY MICHAEL RIVERA.

REPORT OF THE TREASURER: $ 4,311.06 IN THE BANK AFTER DEDUCTING THE "COMO'S" ITALIAN LUNCH ACCEPTED BY DAVID HALPERIN, SECONDED BY NORBERT MILES.

REPORT OF THE CERTIFICATION COMMITTEE: MICHAEL RIVERA WILL APPLY FOR CBRE AND CBNT CERTIFICATIONS. WE WILL REINBURSE

REPORT OF THE MEMBERSHIP COMMITTEE: TO SEND APPLICATION TO DAVID GRICE . HE OFFERED TO HAVE HIS ALAMOGORDO RADIO STATIONS GROUP AS SUSTAINING MEMBER. FEES WILL REMAIN THE SAME FOR 2023 .

REPORT OF THE FREQUENCY COORDINATOR COMMITTEE: Frequency coordination was contacted by Pitt University Radio for mic freqs at the Sun Bowl.

REPORT OF THE SCHOLARSHIP COMMITTEE NO REPORT.

REPORT OF THE WEBSITE COMMITTEE: NOW 4074 VS. 4035 EQUAL 39 HITS.

REPORT OF THE EAS CHAIRMAN: TEXAS AND NEW MEXICO MONTHLY TESTS WERE FINE. MICHAEL RIVERA, NEW CHIEF OF KLAQ TOKE OVER AS THE CHAPTER EAS CHAIRMAN.

REPORT OF THE PROGRAM COMMITTEE: PRESENTATION FROM RHETT FRAZIER FOR THE FEBRUARY MONTH.

NEW BUSINESS OR ANY ITEMS FOR THE CHAPTER INTEREST
WIL,COORDINATE THE FUTURE "ENNES WORKSHOP" WITN NATIONAL

OTHER. .BRUNO WILL CONDUCT A MEETING WITH TEXAS DOT FIBER DISTRIBUTION.

NEXT MEETING DATE AND LOCATION: FEBRUARY THE 8th IN A ZOOM MODE AT 11:00 AM.

LET'S SEE OUR FACES IN ZOOM !!

FEBRUARY PROGRAM

WE MET AT THE LUBY'S CAFETERIA. THERE WAS NO PRESENTATION

MICHAEL RIVERA, NEW CHIEF ENGGINEER FOR KLAQ, LP1, IS NOW EAS CHAIRMAN, HE GOT HIS NATIONAL SBE MEMBERSHIP.

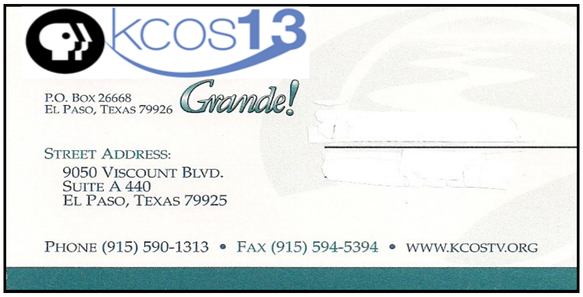
NOW, FOR THIS FEBRUARY 2023 MONTH, WE ARE GOING TO MEET AT YOUR CONVINEANCE, BECAUSE WE ARE DOING "ZOOM" MEETING AND PRESENTATIOM.

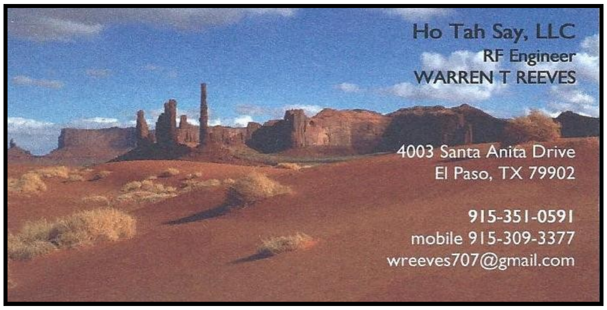
RHETT FRAZIER WILL INTRODUCE *TM TELEVISION*, BROADCAST SYSTEM INTEGRATORS.

WHEN: TUESDAY FEBRUARY THE 8 TH.

WHERE: ZOOM

TIME: 11:30 AM





VMWare

Enterprise software maker VMWare has published a security advisory detailing four flaws affecting its VMware vRealize Log Insight product. Tracked as CVE-2022-31706, the first is a directory traversal vulnerability with a CVSSv3 base score of 9.8. By exploiting the flaw, an unauthenticated, malicious actor could inject files into the operating system of an impacted appliance, resulting in RCE, VMWare says.
Meanwhile, a broken access control RCE vulnerability tracked as CVE-2022-31704 also has a CVCCv3 base score of 9.8. It goes without saying that those impacted by these vulnerabilities should patch as soon as possible.

Oracle

Software giant Oracle has released patches for a whopping 327 security vulnerabilities, 70 of which are rated as having a critical impact. Worryingly, 200 of the issues patched in January can be exploited by a remote unauthenticated attacker.
Oracle is recommending that people update their systems as soon as possible, warning that it has received reports of “attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches.”
In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches, it says.

SAP

SAP’s January Patch Day has seen the release of 12 new and updated security notes. With a CVSS score of 9.0, CVE-2023-0014 is rated as the most severe bug by security firm Onapsis. The flaw affects the majority of all SAP customers and its mitigation is a challenge, Onapsis says.

The capture-replay vulnerability is a risk because it could allow malicious users to obtain access to an SAP system. “Complete patching of the vulnerability includes applying a kernel patch, an ABAP patch, and a manual migration of all trusted RFC and HTTP destinations,” Onapsis explains.

KATE O’ FLAHERTYJAN 31, 2023 7:00 AM