Chapter 38 of the Society of Broadcast Engineers
SBE
EL PASO - LAS CRUCES - JUAREZ

JANUARY
2024

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

NEWS

Google fixes Nearly 100 Android Security Issues

Plus: Apple shuts down a Flipper Zero Attack, Microsoft patches more than 30 vulnerabilities, and more critical updates for the last month of 2023.

December was a hectic month for updates as firms including Apple and Google rushed to get patches out to fix serious flaws in their products before the holiday break.

Enterprise software giants also issued their fair share of patches, with Atlassian and SAP squashing several critical bugs during December.

Here's what you need to know about the important updates you might have missed during the month.

Apple iOS

In mid-December, Apple released iOS 17.2, a major point upgrade containing features such as the Journal app, as well as 12 security patches. Among the flaws fixed in iOS 17.2 is CVE-2023-42890, an issue in the WebKit browser engine that could allow an attacker to execute code.

Another flaw in the iPhone's Kernel, tracked as CVE-2023-4291, could see an app break out of its secure sandbox, Apple wrote on its support page.

Meanwhile, two vulnerabilities in ImageIO, CVE-2023-42898 and CVE-2023-42899, could lead to code execution.

The iOS 17.2 update also put a mechanism in place to prevent a Bluetooth attack using a penetration testing device called Flipper Zero, according to tests by ZDNET and 9to5Mac. The annoying denial of service cyber-assault could cause a flurry of pop ups to appear on an iPhone and eventually lock up the device.

Apple also released iOS 16.7.3, Safari 17.2, macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2, tvOS 17.2 and watchOS 10.2.

Just one week after releasing iOS 17.2, Apple issued iOS 17.2.1 and iOS 16.7.4 for older devices, alongside macOS Sonoma 14.2.1. The surprise iPhone update contains unspecified bug and security fixes, while the macOS patch fixes a single flaw tracked as CVE-2023-42940.

Google Android

The Google Android December Security Bulletin was a hefty one, fixing nearly 100 security issues. The update includes patches for two critical issues in the Framework, the most severe of which could lead to remote escalation of privilege with no additional privileges needed. User interaction is not needed for exploitation, Google said.

CVE-2023-40088 is a critical flaw in the system that could lead to remote code execution, while CVE-2023-40078 is an elevation of privilege bug rated as having a high impact.

Google has also issued an update for its smart device WearOS platform, fixing CVE-2023-40094, an elevation of privilege flaw. The Pixel Security Bulletin has not been posted at the time of writing.

Continues in page 2

KTSM-TV

KVIA-TV

KRWG-TV

KBNA-AM/FM & KAMA-AM

KHEY-AM/FM, KPRR-FM &
KTSM-AM/FM

KLAQ-FM, KISS-FM &
KROD-AM

KPAS-FM-
ALGIE A. FELDER CSBE

KINT98.COM
INTERNET RADIO NETWORK

BURST COMMUNICATIONS
INC.- KIRK BASEFSKY

JOHN LACKNESS

ENTRAVISION
COMMUNICATIONS

SCMS, INC.-

ABS ADVANCED BROADCAST
SERVICES, LLC

KSCE-TV

RF Specialties of Texas

KCOS-TV

KELP-AM
ARNOLD McClatchy.

MARSAND,INC.

Ho Tah Say. LLC

Google Chrome

Google ended a bumper December of updates in style with an emergency fix for its Chrome browser. The eighth zero-day vulnerability impacting Chrome in 2024, CVE-2023-7024 is a heap buffer overflow issue in the open source WebRTC component. Google is “aware that an exploit for CVE-2023-7024 exists in the wild,” the browser maker said in an advisory.

It wasn’t the first fix released by Google in December. The software giant also issued a Chrome patch mid-month to fix nine security issues. Of the flaws reported by external researchers, five are rated as having a high severity, including CVE-2023-6702, a type confusion flaw in V8, and four use-after-free bugs.

Earlier in the month
Google released Chrome 120, fixing 10 security flaws, including two rated as having a high severity. CVE-2023-6508 is a use-after-free bug in Media Stream, while CVE-2023-6509 is a use-after-free issue in Side Panel Search.

Microsoft

Microsoft’s December Patch Tuesday fixes over 30 vulnerabilities, including several remote code execution (RCE) flaws. Among the critical fixes is CVE-2023-36019, a spoofing vulnerability in Microsoft Power Platform Connector with a CVSS score of 9.6. The issue could see an attacker manipulate a malicious link, app, or file to trick the victim. However, you would have to click on a specially crafted URL to be compromised.

Meanwhile, CVE-2023-35628 is a Windows MSHTML Platform RCE bug rated as critical with a CVSS score of 8.1. “The attacker could exploit this vulnerability by sending a specially crafted email which triggers automatically when it is retrieved and processed by the Outlook client,” Microsoft said, adding that this could lead to exploitation before the email is viewed in the Preview Panel.

Continues 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 COORDINATION 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 121/12/2023 LOCATION: ANGRY OWL RESTAURANT

MEETING CALLED TO ORDER: 12:26 P.M. , BY ANTONIO CASTRO. WE WERE 6 (SIX) ATTENDANTS

REPORT OF THE SECRETARY: MINUTES ON DECEMBER NEWSLETTER. ACCEPTED BY NORBERT MILES, SECONDED BY DAVID HALPERIN.

REPORT OF THE TREASURER: $ 2,264.89 IN THE BANK. ACCEPTED BY NORBERT MILES, SECONDED BY WALTER HANTHORN.

REPORT OF THE CERTIFICATION COMMITTEE: WAITING FOR FIVE STUDENTS OF RIVERSIDE HIGH SCHOOL TO GET ***CTO***.

REPORT OF THE MEMBERSHIP COMMITTEE: GLENN LEFFLER WAITING FOR **KELP** NEWOWNER IN ORDER TO RENEW THEIR MEMBERSHIP. BRUNO CRUZ TO INVITE KFOX-KDBC AS SUSTAINING MEMBERSHIP FOR 2024 AND ELIAS VENTANILLA TO INVITE “TELEMUNDO 48” AS WELL .

REPORT OF THE FREQUENCY COORDINATOR COMMITTEE: ***NO REPORT***

REPORT OF THE SCHOLARSHIP COMMITTEE: NO FOUNDS THIS YEAR.

REPORT OF THE WEBSITE COMMITTEE: NOW 4748 VS. 4722 EQUAL 26 HITS.

REPORT OF THE EAS CHAIRMAN: TEXAS MONTHLY TESTS WAS FINE. NEW MEXICO CAME TWO DAYS LATER

REPORT OF THE PROGRAM COMMITTEE: NO REPORT.

NEW BUSINESS OR ANY ITEMS FOR THE CHAPTER INTEREST :: NONE.

OTHER. NONE

NEXT MEETING DATE AND LOCATION: JANUARY THE 9TH. TIME: 10:30 AM IN A ZOOM CALL FROM ANTONIO’S.

MEETING ADJOURNED: AT 12:49 P.M.

It is Collecting times for memberships. Let’s start 2024 financially right . Square invoices to follow !!

JANUARY PROGRAM

THE DECEMBER CHAPTER 38 MEETING WAS HELD AT “THE ANGRY OWL” RESTAURANT.

WE HAD AN ATTENDANCE OF 6 (SIX) ENGINEERS, RADIO AND TV

OUR JANUARY MEETING WILL BE IN THE ZOOM MODE AND THERE IS NO PRESENTATION.

WE NEED TO ELECT NEW OFFICERS !

WHEN:

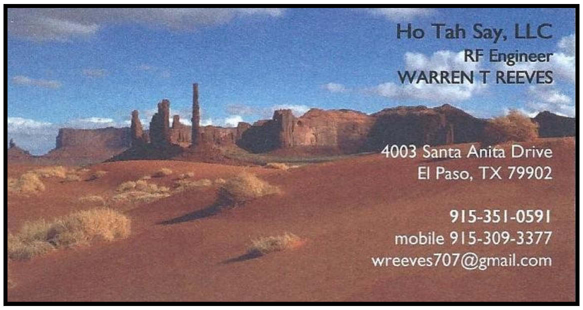
JANUARY 9 TUESDAY.

WHERE:

ZOOM AT ANTONIO’S

TIME:

10:30 AM



It was a fairly light Patch Tuesday, and none of the issues fixed in the month's update cycle are known to have been exploited, but it still makes sense to apply the fixes as soon as you can.

Mozilla Firefox

Mozilla has fixed 18 security vulnerabilities in its Firefox browser, a third of which are rated as having a high severity. Of these, CVE-2023-6856 is a heap-buffer-overflow issue affecting WebGL DrawElementsInstanced method with Mesa VM driver that could allow an attacker to perform remote code execution and sandbox escape.
Meanwhile, Mozilla has also fixed memory safety bugs tracked as CVE-2023-6864 and CVE-2023-6873. "Some of these bugs showed evidence of memory corruption and we presume that with enough effort [they] could have been exploited to run arbitrary code," Mozilla said.

Apache

The Apache Software Foundation has issued a patch for a flaw in its Struts 2 open source developer framework. Tracked as CVE-2023-50164, the issue is rated as critical with a CVSS score of 9.8.
Using the vulnerability, an attacker could manipulate file upload parameters to enable paths traversal. Under some circumstances, this could lead to uploading a malicious file and be used to perform RCE, according to a security advisory.
To fix the flaw, it's important to upgrade to Struts 2.5.33 or Struts 6.3.0.2 as soon as possible.

Atlassian

Enterprise software giant Atlassian has issued a patch to fix critical RCE vulnerabilities in its Confluence Data Center and Server. Tracked as CVE-2023-22522, the template injection vulnerability allows an authenticated attacker to inject unsafe user input into a Confluence page. "Using this approach, an attacker is able to achieve RCE on an affected instance," Atlassian said in an advisory.

Marked as critical with a CVSS score of 9, the bug affects all versions including and after 4.0.0 of Confluence Data Center and Server. Atlassian "recommends patching to the latest version or a fixed LTS version" to address the issue.
Other patches released by Atlassian during the month include a fix for an RCE vulnerability in the Atlassian macOS app, an RCE bug in Assets Discovery, and a SnakeYAML library RCE issue impacting multiple products.

SAP

Business software maker SAP has released its December Security Patch Day, fixing several serious security flaws. The most critical, with a CVSS score of 9.1, are four escalation-of-privilege bugs in SAP Business Technology Platform tracked as CVE-2023-49583, CVE-2023-50422, CVE-2023-50423, and CVE-2023-50424.

"It allows an unauthenticated attacker to obtain arbitrary permissions within the application leading to high impact on the application's confidentiality and integrity," security firm Onapsis said.
Meanwhile, CVE-2023-42481 is an improper access control vulnerability in SAP Commerce Cloud with a CVSS score of 8.1. "This allows a user who is actually blocked to regain access to the application, leading to considerable impact on confidentiality and integrity," according to Onapsis.