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

NOVEMBER 2022

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

NEWS

Update Chrome, zoom and Windows Right Now

Plus: Important patches from Apple, VMWare, Cisco, Zimbra, SAP, and Oracle.

UPDATES HAVECONTINUED to be released thick and fast in October, with patches now available from the likes of Apple for iOS, Google Chrome, Android, and, of course, Microsoft in its monthly Patch Tuesday. That's in addition to updates to fix issues in Zoom, Cisco, VMWare, and SAP products.
Here are the details about all the important patches issued in October

Apple iOS 16.1 and iPadOS 16
October saw the release of two iOS 16 versions following the launch of the iPhone maker's updated operating system in September. First came iOS 16.0.3, which fixed some teething issues, including several bugs as well as a security flaw in Mail that could allow denial of service attacks.

Only weeks later, Apple released iOS 16.1 and iPadOS 16—the latter of which was delayed to coincide with the launch of the latest iPad models. The latest iOS versions come with a much longer list of security fixes and include an already exploited flaw.

Tracked as CVE-2022-42827, the kernel vulnerability could allow an application to execute code with kernel privileges, according to Apple's support page. The operating system update fixes 20 vulnerabilities in total, including three in the kernel at the heart of the iPhone's operating system. Meanwhile, iOS 16.1 fixes four flaws in WebKit, the engine that powers the Safari browser, two of which could lead to code execution if exploited.

Apple has also released iOS 15.7.1 and iPadOS 15.7.1 which fix the already exploited kernel flaw. Given the seriousness of the issues and the lack of detail provided, it's a good idea to update to iOS 16.1 or iOS 15.7.1 as soon as possible.

Microsoft Patch Tuesday
Patch Tuesday has once again arrived along with fixes for a rather hefty list of 84 flaws. Of these, 13 are rated as critical, and one is being used in attacks. Tracked as CVE-2022-41033, the elevation of privilege vulnerability in Windows COM+ Event System Service impacts almost every version of Windows. The flaw is serious, as it could be chained with other exploits to take over someone's machine.
Notably absent from the Patch Tuesday updates was a fix for two actively exploited bugs tracked as CVE-2022-41040 and CVE-2022-41082, known as ProxyNotShell.

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

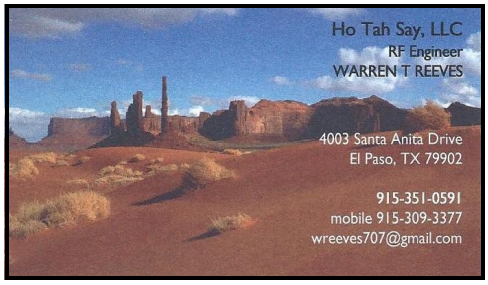
RF Specialties of Texas

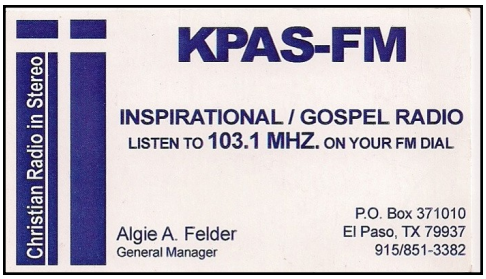
KCOS-TV

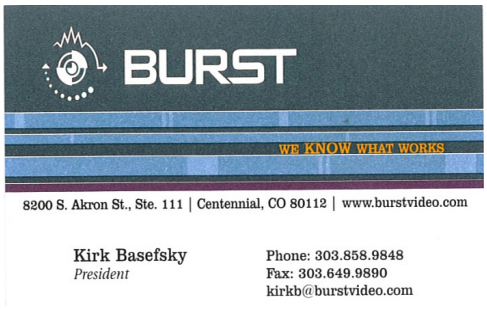
KELP-AM
ARNOLD McClatchy.

MARSAND,INC.

Ho Tah Say. LLC







The flaws were reported to Microsoft by security vendor GTSC. Microsoft has shared mitigations, but researchers warn they can be bypassed.

Google Chrome

October saw another emergency update for Google Chrome users, with the browser maker issuing a fix for a type confusion flaw in the V8 JavaScript engine tracked as CVE-2022-3723. The issue was patched within days of being reported by Avast researchers, which is indicative of how serious it is: The flaw could be exploited to execute code and gain control of the system. Google said it is “aware of reports that an exploit for CVE-2022-3723 exists in the wild.” Earlier in the month, Google released Chrome 106, patching six vulnerabilities ranked as high-severity. Notable flaws include CVE-2022-3445, a use-after-free bug in Skia, the open source 2D graphics library that serves as the graphics engine for Google Chrome.
Other issues fixed in October are a heap buffer overflow in WebSQL tracked as CVE-2022-3446 and a use-after-free bug in Permissions API tracked as CVE-2022-3448, Google wrote in its blog. Google also fixed two use-after-free bugs in Safe Browsing and in Peer Con-nection.

Cisco

Cisco has urged companies to patch two flaws in its AnyConnect Secure Mobility Client for Windows after it was confirmed the vulnerabilities are being used in attacks.

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:
David Halperin

EXECUTIVE COMMITTEE:
Antonio Castro
Bruno Cruz
Walter Hanthorn

ABS
Advanced Broadcast Services LLC
Providing world class engineering and tower services to the broadcast and telecommunications industries.
David Grice
President
915-308-1227
6776 Villa Hermosa Dr
El Paso TX 79912
www.AdvancedBroadcastServices.com
Dgrice@AdvancedBroadcastServices.com

FEDERAL COMMUNICATIONS COMMISSION

NM STATE
KRWG PUBLIC MEDIA
npr

SCMS INC.
YOU KNOW WE KNOW RADIO
for Broadcast Equipment Solutions
NEW
USED
RENTALS
TRADE-INS
800 438 6040 Sales
704 889 4508
www.scmsinc.com

iHeart MEDIA
Walter Alvarez
Market President | El Paso
iHeartMedia
4045 N Mesa Street
El Paso, TX 79902
o 915.351.5473
m 915.201.7627
walteralvarez@iheartmedia.com

EAS
Emergency Alert System

EL PASO, TX SBE CHAPTER 38 MEETING MINUTE

DATE 10/11/2022 LOCATION: MICROSOFT TEAMS

MEETING CALLED TO ORDER: 10:52 AM, BY ANTONIO CASTRO. WE WERE ONLY 13 (THIRDTEEN) ATTENDANTS

REPORT OF THE SECRETARY: MINUTES IN THE OCTOBER NEWS-LETTER. ACCEPTED BY NBORBERT MILES, SECONDED BY NOE ROD-RIGUEZ

REPORT OF THE TREASURER: $ 4,621.26 IN THE BANK. ACCEPTED BY OWEN SMITH, SECONDED BY JERRY BUTLER.

REPORT OF THE CERTIFICATION COMMITTEE: NO REPORT.

REPORT OF THE MEMBERSHIP COMMITTEE: STILL DAVID GRICE OFFER TO HAVE HIS ALAMOGORDO RADIO STATIONS GROUP AS SUSTAINING MEMBER. .

REPORT OF THE FREQUENCY COORDINATOR COMMITTEE: NO REPORT.

REPORT OF THE SCHOLARSHIP COMMITTEE NO REPORT.

REPORT OF THE WEBSITE COMMITTEE: NOW 3942 VS. 3918 EQUAL 24 HITS.

REPORT OF THE EAS CHAIRMAN: TEXAS MONTHLY TEST WAS FINE, NEW MEXICO WAS NOR RECEIVED BY KLAQ THUS NOT RE-LAYED.

REPORT OF THE PROGRAM COMMITTEE: ACTUS PRESENTATION AND DEMOSTRATION WAS GREAT IN THE MICROSOFT TEAMS..

NEW BUSINESS OR ANY ITEMS FOR THE CHAPTER INTEREST: TRAM WAY FROM KFOX NOW IN GOOD SHAPE.

OTHER. .NONE.

NEXT MEETING DATE AND LOCATION: NOVEMBER 08 AT 11 AM FOR A ZOOM PRESENTATION.

MEETING ADJOURNED: AT 11:04 AM PM.

NOVEMBER PROGRAM

FOR LAST MONTH OF OCTOBER, WE HAD OUR REGULAR MEETING IN THE "ZOOM" MODE.

OUR GUEST THIS TIME WAS KEN RUBIN FROM ACTUS DIGITAL. HE AND HIS GUEST DEMONSTATED THEIR MARKET-LEADING QUALITY MONI-TORING AND COMPLIANCE LOGGING PLATFORM.

THEY SHOWED THE OTT STREAMING AND A SNEAK-PEEK AT ACTUS V8.5 ANNOUNCED AT IBC IN SEPTEMBER WITH THE LATEST IN OTT QUALITY MONITORING.

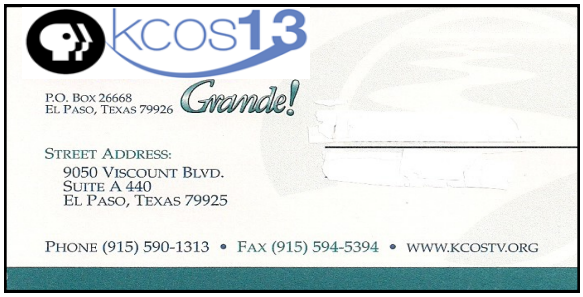
NOW, FOR THIS NOVEMBER MONTH, WE ARE GOING TO HAVE A ZOOM MODE CHAPTER MEETING

WHEN: TUESDAY NOVEMBER THE 8TH

WHERE: AT YOUR PC OR CEL PHONE

TIME: 10:30 AM FOR WELCOME AND CHAT AND THEN, 11:00 AM MEETING WILL SART.

WE WILL INTRODUCE A GUEST FROM LAS CRUCES, NM



Tracked as CVE-2020-3433, the first could allow an attacker with valid credentials on Windows to execute code on the affected machine with system privileges.
Meanwhile, CVE-2020-3153 could allow an attacker with valid Windows credentials to copy malicious files to arbitrary locations with system-level privileges.
Meanwhile, CVE-2020-3153 could allow an attacker with valid Windows credentials to copy malicious files to arbitrary locations with system-level privileges.

The US Cybersecurity and Infrastructure Security Agency has added the Cisco flaws to its already exploited vulnerabilities catalog.
While both the Cisco flaws require the attacker to be authenticated, it's still important to update now.

Zoom

Video conferencing service Zoom patched several issues in October, including a flaw in its Zoom client for meetings, which is marked as having a high severity with a CVSS Score of 8.8. Zoom says versions before version 5.12.2 are susceptible to a URL-parsing vulnerability tracked as CVE-2022-28763.
"If a malicious Zoom meeting URL is opened, the link may direct the user to connect to an arbitrary network address, leading to additional attacks including session takeovers," Zoom said in a security bulletin.

Earlier in the month, Zoom alerted users that its client for meetings for macOS starting with 5.10.6 and prior to 5.12.0 contained a debugging port misconfiguration.

VMWare

Software giant VMWare has patched a serious vulnerability in its Cloud Foundation
Tracked as CVE-2021-39144. The remote code execution vulnerability via XStream open source library is rated as having a critical severity with a maximum CVSSv3 base score of 9.8. "Due to an unauthenticated endpoint that leverages XStream for input serialization in VMware Cloud Foundation, a malicious actor can get remote code execution in the context of 'root' on the appliance," VMWare said in an advisory.
The VMware Cloud Foundation update also addresses an XML External Entity vulnerability with a lesser CVSSv3 base score of 5.3. Tracked as CVE-2022-31678, the bug could allow an unauthenticated user to perform denial of service.

Zimbra

Software firm Zimbra has issued patches to fix an already-exploited code execution flaw that could allow an attacker to access user accounts. The issue, tracked as CVE-2022-41352, has a CVSS severity score of 9.8.
Exploitation was spotted by Rapid7 researchers, who identified signs it had been used in attacks. Zimbra initially released a workaround to fix it, but now the patch is available, you should apply it ASAP.

SAP

Enterprise software firm SAP has published 23 new and updated Security Notes in its October Patch Day. Among the most serious issues is a critical Path Traversal vulnerability in SAP Manufacturing Execution. The vulnerability affects two plugins: Work Instruction Viewer and Visual Test and Repair and has a CVSS score of 9.9.
Another issue with a CVSS score of 9.6 is an account hijacking vulnerability in the SAP Commerce login page.

Oracle

Software giant Oracle has released a whopping 370 patches as part of its quarterly security update. Oracle's Critical Patch Update for October fixes 50 vulnerabilities rated as critical.
The update contains 37 new security patches for Oracle MySQL, 11 of which may be remotely exploitable without authentication. It also contains 24 new security patches for Oracle Financial Services Applications, 16 of which may be remotely exploitable without authentication.
Due to "the threat posed by a successful attack," Oracle "strongly recommends" that customers apply Critical Patch Update security patches as soon as possible.