NEWS

UPDATE WNDOWS NOW!

Plus: Google issues fixes for Android bugs. And Cisco, Citrix, SAP, WordPress, and more issue major patches for enterprise systems.

JUNE HAS SEEN the release of multiple security updates, with important patches issued for the likes of Google's Chrome and Android as well as dozens of patches for Microsoft products, including fixes for a Windows zero-day vulnerability that attackers had already exploited. Apple updates were absent at the time of writing, but the month also included some major enterprise-focused patches for Citrix, SAP, and Cisco products.

Here's what you need to know about the major patches released in the past month.

Microsoft

Microsoft's Patch Tuesday release was pretty hefty in June, including fixes for 55 flaws in the tech giant's products. This Patch Tuesday was particularly important because it addressed an already exploited remote code execution (RCE) issue in Windows dubbed Follina, which Microsoft has been aware of since at least May.

Tracked as CVE-2022-30190, Follina—which takes advantage of vulnerabilities in the Windows Support Diagnostic tool and can execute without the need to open a document—has already been used by multiple criminal groups and state-sponsored attackers.
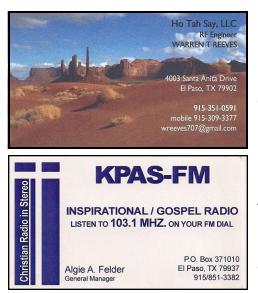
Three of the vulnerabilities addressed in Patch Tuesday affecting Windows Server are RCE flaws and rated as critical. However, the patches seem to be breaking some VPN and RDP connections, so be careful.

Google Chrome

Google Chrome updates continue to come thick and fast. That's no bad thing, as the world's most popular browser is by default one of the biggest targets for hackers. In June, Google released Chrome 103 with patches for 14 vulnerabilities, some of which are serious.

Tracked as CVE-2022-2156, the biggest flaw is a use-after-free issue in Base reported by Google's Project Zero bug-hunting team that could lead to arbitrary code execution, denial of service, or corruption of data. Worse, when chained with other vulnerabilities the flaw could lead to full system compromise.

Other issues patched in Chrome include vulnerabilities in Interest Groups, WebApp Provider, and a flaw in the V8 Javascript and WebAssembly engine.

Google Android

Of the multiple Android security Issues Google patched in June, the most severe is a critical security vulnerability in the System component that could lead to remote code execution with no additional execution privileges needed, Google said in its Android Security Bulletin.

Google also released updates for its Pixel devices to patch issues in the Android Framework, Media Framework, and System Components.

Samsung users seem to have gotten lucky with Android updates of late, with the device maker rolling out its patches very quickly. The June security update is no different, reaching the Samsung Galaxy Tab S7 series, Galaxy S21 series, Galaxy S22 series, and the Galaxy Z Fold 2 straightaway.

Cisco

Software maker Cisco released a patch in June to fix a critical vulnerability in Cisco Secure Email and Web Manager and Cisco Email Security Appliance that could allow a remote attacker to bypass authentication and log in to the web management interface of an affected device.

The issue, tracked as CVE-2022-20798, could be exploited if an attacker enters something specific on the login page of the affected device, which would provide access to the web-based management interface, Cisco said.

EL PASO, TX   SBE CHAPTER 38   MEETING MINUTE

DATE 6/15/2022   LOCATION: ZOOM ANTONIO

MEETING CALLED TO ORDER: 11:00 AM, BY ANTONIO CASTRO. THERE WERE ONLY 15 (FIFTEEN) ATTENDANTS

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

REPORT OF THE TREASURER: $ 4,729.10 IN THE BANK , ACCEPTED BY BRUNO CRUZ, SECONDED BY MARIO TELLEZ.

REPORT OF THE CERTIFICATION COMMITTEE: DAVID HALPERIN IS DOING A REVISION TO PROCEDURES.

REPORT OF THE MEMBERSHIP COMMITTEE: DAVID GRICE OFFER TO HAVE HIS ALAMOGORDO RADIO STATIONS GROUP AS SUSTAINING MEMBER. BRAD BISHOP REINSTATED TO KFOX TV.

REPORT OF THE FREQUENCY COORDINATOR COMMITTEE: IT IS AN ISSUE WITH THE MEXICAN (CD. JUAREZ) WITH CHANEL 14-1, CONFUSING THE BRANDING OF KFOX OWN.INVESTIGATIONWILL FOLLOW.

REPORT OF THE SCHOLARSHIP COMMITTEE $ 1,000.00 CHECK WAS PRESENTED TO THE STUDENT **YUDITH CAMPOS** AS 2022 SCHOLARSHIP.

REPORT OF THE WEBSITE COMMITTEE: NOW 3707 VS. 3659 EQUAL 48 HITS. WILL CONTEMPLATE THE SBE.ORG AS OUR DOMAIN NAME.

REPORT OF THE EAS CHAIRMAN: MONTHLY TEXAS TEST WAS FINE WHILE THE NEW MEXICO WAS DROPPED FROM THE KKOB-AM

REPORT OF THE PROGRAM COMMITTEE: JAVIER RUANO FROM TELEVEZ DID THE PRESENTATION. GOOD STUFF.

NEW BUSINESS OR ANY ITEMS FOR THE CHAPTER INTEREST: TRAM WAY FROM KFOX WILL START OPERATING THIS MONTH.
 .
OTHER   REBATE CHECK RECEIVED FROM SBE NATIONAL.

NEXT MEETING DATE AND LOCATION: JULY 12 AT NOON. PLACE: LUBY'S RESTAURANT, UTEP.

YUDITH CAMPOS RX SCHOLARSHIP

JULYY PROGRAM

FOR LAST MONTH OF JUNE, WE HAD OUR REGULAR MEETING IN THE ZOOM MODE AND THE PRESENTA-TION WAS FROM JAVIER RUANO, GENERAL MANAGER FROM TELEVEZ USA LLC. HE SHOWED THE "HEXYLON -A"
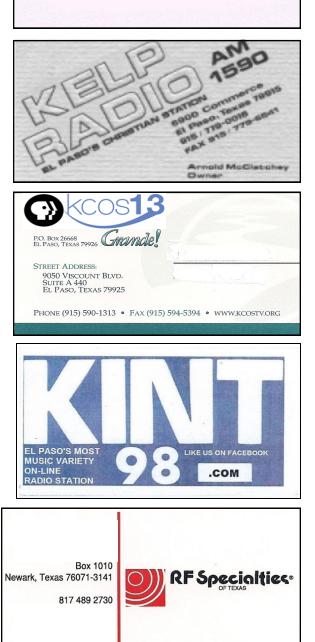
_____

NOW, FOR THIS JULY MONTH, WE ARE GOING TO HAVE A LIVE CHAPTER MEETING (BACK TO NORMAL) AND YOU CAN HAVE VACATIONS BECAUSE WE DELAYED ONE WEEK

WHEN: TUESDAY JULY 19 TH

WHERE: CAFETERIA LUBY'S (UTEP)

TIME: 12:00 PM (NOON).

IF WE GET A PRESENTER, YOU WILL BE NOTIIFIED.

HAVE A GREAT TIME !!

KLAQ 95.5FM KROD 600AM
BRAD DUBOW
GENERAL MANAGER
4180   N.Mesa   El Paso, Tx 79912
(915) 544-9550

KELP RADIO AM 1590
EL PASO'S CHRISTIAN STATION
6900 Commerce
El Paso, Texas 79915
915 / 779-0016
FAX 915 / 779-6941
Arnold McClatchey
Owner

kcos13 Grande!
P.O. Box 26668
El Paso, Texas 79926
STREET ADDRESS:
9050 VISCOUNT BLVD.
SUITE A 440
EL PASO, TEXAS 79925
PHONE (915) 590-1313 • FAX (915) 594-5394 • WWW.KCOSTV.ORG

KINT 98
EL PASO'S MOST MUSIC VARIETY ON-LINE RADIO STATION
LIKE US ON FACEBOOK
.COM

Box 1010
Newark, Texas 76071-3141
817 489 2730
RF Specialties OF TEXAS

Citrix

Citrix has issued a warning urging users to patch some major vulnerabilities that could let attackers reset admin passwords. The vulnerabilities in Citrix Application Delivery Management could result in corruption of the system by a remote, unauthenticated user, Citrix said in a security bulletin. "The impact of this can include the reset of the administrator password at the next device reboot, allowing an attacker with ssh access to connect with the default administrator credentials after the device has rebooted," the company wrote.

Citrix recommends that traffic to the Citrix ADM's IP address be segmented from standard network traffic. This diminishes the risk of exploitation, it said. However, the vendor also urged customers to install the updated versions of Citrix ADM server and Citrix ADM agent "as soon as possible."

SAP

Software firm SAP has released 12 security patches as part of its June Patch Day, three of which are serious. The first listed by SAP relates to an update released on April 2018 Patch Day and applies to the browser control Google Chromium used by the firm's business clients. Details of this vulnerability aren't available, but it has a severity score of 10, so the patch should be applied straightaway.

Another major fix concerns an issue in the SAProuter proxy in NetWeaver and ABAP Platform, which could allow an attacker to execute SAProuter administration commands from a remote client. The third major patch fixes a privilege escalation bug in SAP PowerDesigner Proxy 16.7.

Splunk Enterprise

Splunk has released some out-of-band patches for its Enterprise product, fixing issues including a critical-rated vulnerability that could lead to arbitrary code execution.

Labeled CVE-2022-32158, the flaw could allow an adversary to compromise a Universal Forwarder endpoint and execute code on other endpoints connected to the deployment server. Thankfully, there's no indication that the vulnerability has been used in any real-world attacks.

Ninja Forms WordPress Plug-In

Ninja Forms, a WordPress plug-in with over a million active installations, has patched a serious issue that's probably being used by attackers in the wild. "We uncovered a code injection vulnerability that made it possible for unauthenticated attackers to call a limited number of methods in various Ninja Forms classes, including a method that unserialized user-supplied content, resulting in Object Injection," security analysts at the WordPress Wordfence Threat Intelligence team said in an update.

This could allow attackers to execute arbitrary code or delete arbitrary files on sites where a separate POP chain was present, researchers said.

The flaw has been fully patched in versions 3.0.34.2, 3.1.10, 3.2.28, 3.3.21.4, 3.4.34.2, 3.5.8.4, and 3.6.11. WordPress appears to have performed a forced automatic update for the plug-in, so your site may already be using one of the patched versions.

Atlassian

Australian software company Atlassian has released a patch to fix a zero-day flaw that's already being exploited by attackers. Tracked as CVE-2022-26134, the RCE vulnerability in the Confluence Server and Data Center can be used to backdoor internet-exposed servers.

GitLab

GitLab has issued patches for versions 15.0.1, 14.10.4, and 14.9.5 for GitLab Community Edition and Enterprise Edition. The updates contain important security fixes for eight vulnerabilities, one of which could allow for account takeover.

With this in mind, the firm "strongly recommends" that all GitLab installations be upgraded to the latest version "as soon as possible." GitLab.com is already running the patched version.