Your Security Rabbits report for April 15, 2022

Hot topics

Nothing today

News

Blog â€“ Flashpoint

1,701 New Vulnerabilities: Vulnerability Intelligence Infographic, March 2022: Key Trends and Analysis

According to Risk Based Security, a Flashpoint company, 1,701 new vulnerabilities were disclosed last month, with 22 percent (382) of them missed by CVE/NVD. Here are some things you should know about the full vulnerability picture. Apple zero-days are still at large Among the vulnerabilities missed by MITRE and NIST are CVE-2022-22674 and CVE-2022-22675, two […] The post 1,701 New Vulnerabilities: Vulnerability Intelligence Infographic, March 2022: Key Trends and Analysis appeared first on Flashpoint.

Security Affairs

Analysis of the SunnyDay ransomware

The analysis of a recent sample SunnyDay ransomware revealed some similarities with other ransomware, such as Ever101, Medusa Locker, Curator, and Payment45. Seguranca-Informatica published an analysis of a recent sample of SunnyDay ransomware. As a result of the work, some similarities between other ransomware samples such as Ever101, Medusa Locker, Curator, and Payment45 were found. […] The post Analysis of the SunnyDay ransomware appeared first on Security Affairs.

Cyware News - Latest Cyber News

Campaign Similar to Operation Kitty Phishing Found Targeting South Koreans

According to researchers, the campaign was first observed in April and aims to steal data from individuals in South Korea. They are targeted via spear-phishing emails that include malicious Word documents.

Cyware News - Latest Cyber News

CISA Issues Warning About Malicious Tools Targeting ICS/SCADA Devices

The advisory highlights that OPC Unified Architecture (OPC UA) servers and multiple versions of Programmable Logic Controllers (PLCs) from Schneider Electric, and OMRON are vulnerable to such attacks.

The Hacker News

Critical Auth Bypass Bug Reported in Cisco Wireless LAN Controller Software

Cisco has released patches to contain a critical security vulnerability affecting the Wireless LAN Controller (WLC) that could be abused by an unauthenticated, remote attacker to take control of an affected system. Tracked as CVE-2022-20695, the issue has been rated 10 out of 10 for severity and enables an adversary to bypass authentication controls and log in to the device through the

Security Affairs

Critical VMware Workspace ONE Access CVE-2022-22954 flaw actively exploited

Threat actors are actively exploiting a critical vulnerability in VMware Workspace ONE Access and Identity Manager recently patched by the vendor. Threat actors are actively exploiting a critical flaw, tracked as CVE-2022-22954, in VMware Workspace ONE Access and Identity Manager recently patched by the vendor. Researchers from cyber threat intelligence BadPackets also reported that the vulnerability […] The post Critical VMware Workspace ONE Access CVE-2022-22954 flaw actively exploited appeared first on Security Affairs.

The Hacker News

Ethereum Developer Jailed 63 Months for Helping North Korea Evade Sanctions

A U.S. court has sentenced former Ethereum developer Virgil Griffith to five years and three months in prison and pay a $100,000 fine for conspiring with North Korea to help use cryptocurrencies to circumvent sanctions imposed on the country. "There is no question North Korea poses a national security threat to our nation, and the regime has shown time and again it will stop at nothing to ignore

Feds: APTs Have Tools That Can Take Over Critical Infrastructure

Cyware News - Latest Cyber News

A Vulnerability in Apache Struts Could Allow for Remote Code Execution

A vulnerability has been discovered in Apache Struts, which could allow for remote code execution. Apache Struts is an open-source framework used for building Java web applications.

The Hacker News

As State-Backed Cyber Threats Grow, Here's How the World Is Reacting

With the ongoing conflict in Eurasia, cyberwarfare is inevitably making its presence felt. The fight is not only being fought on the fields. There is also a big battle happening in cyberspace. Several cyber-attacks have been reported over the past months. Notably, cyber attacks backed by state actors are becoming prominent. There have been reports of a rise of ransomware and other malware

Security Affairs

CISA adds Windows CLFS Driver Privilege Escalation flaw to its Known Exploited Vulnerabilities Catalog

The U.S. CISA added the CVE-2022-24521 Microsoft Windows CLFS Driver Privilege Escalation Vulnerability to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the CVE-2022-24521 privilege escalation vulnerability in Microsoft Windows Common Log File System (CLFS) Driver. According to Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, FCEB […] The post CISA adds Windows CLFS Driver Privilege Escalation flaw to its Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Cyware News - Latest Cyber News

Cisco's Webex phoned home audio telemetry even when muted

Researchers at two US universities have found that muting popular native video-conferencing apps fails to disable device microphones - and that these apps have the ability to access audio data when muted, or actually do so.

The Hacker News

Critical VMware Cloud Director Bug Could Let Hackers Takeover Entire Cloud Infrastructure

Cloud computing and virtualization technology firm VMWare on Thursday rolled out an update to resolve a critical security flaw in its Cloud Director product that could be weaponized to launch remote code execution attacks. The issue, assigned the identifier CVE-2022-22966, has a CVSS score of 9.1 out of a maximum of 10. VMware credited security researcher Jari Jaaskela with reporting the flaw. <

IC3.gov News

Cybercriminals Trick Victims into Transferring Funds to "Reverse" Instant Payments

Cyware News - Latest Cyber News

Experts warn of concerns around Microsoft RPC bug

Windows hosts running the Server Message Block protocol (SMB protocol) are vulnerable to this bug. SMB protocols allow users to share access to files and tools on remote servers.

Google Chrome emergency update fixes zero-day used in attacks

Threatpost

Threat actors have developed custom modules to compromise various ICS devices as well as Windows workstations that pose an imminent threat, particularly to energy providers.

The Hacker News

Google Releases Urgent Chrome Update to Patch Actively Exploited Zero-Day Flaw

Google on Thursday shipped emergency patches to address two security issues in its Chrome web browser, one of which it says is being actively exploited in the wild. Tracked as CVE-2022-1364, the tech giant described the high-severity bug as a case of type confusion in the V8 JavaScript engine. Clement Lecigne of Google's Threat Analysis Group has been credited with reporting the flaw on April 13

Cyware News - Latest Cyber News

Hafnium's New Malware Hides Behind Scheduled Tasks

Microsoft linked the Chinese-backed Hafnium group to a defense evasion malware Tarrask used by cybercriminals to attain persistence on compromised Windows environments. Researchers uncovered a recent malicious activity wherein hackers abused an unpatched zero-day vulnerability for their initial attack vectors. Experts suggest finding these hidden tasks by closer manual inspection of the Windows Registry and looking for scheduled tasks without an SD Value within their Task Key.

CyberScoop

Information-stealing malware is spreading widely on Telegram, Cisco Talos says

The ZingoStealer information stealer identified by Cisco Talos threat analysts can exfiltrate credentials and steal cryptocurrency wallet information. The post Information-stealing malware is spreading widely on Telegram, Cisco Talos says appeared first on CyberScoop.

ZDNet | security RSS

Meet ZingoStealer: the Haskers Gang's new, free malware

ZingoStealer is able to spread cryptocurrency mining malware.

Cyware News - Latest Cyber News

Pipedream, an extremely versatile malware toolkit, could be used for targeting power grids, refineries, and other ICS systems

The United States government has issued an advisory for the malware toolkit dubbed Pipedream that cybercriminal groups could use to potentially target all critical infrastructure owners worldwide.

Naked Security

S3 Ep78: Darkweb hydra, Ruby, quantum computing, and a robot revolution [Podcast]

Latest episode - listen now!

CyberScoop

Treasury updates Lazarus Group sanctions with digital currency address linked to Ronin Bridge hack

The address received $600 million in Ethereum and other digital currency during the March attack, crypto-tracking company Chainalysis said. The post Treasury updates Lazarus Group sanctions with digital currency address linked to Ronin Bridge hack appeared first on CyberScoop.

Security Affairs

US gov agencies e private firms warn nation-state actors are targeting ICS & SCADA devices

The US government agencies warned of threat actors that are targeting ICS and SCADA systems from various vendors. The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) published a joint Cybersecurity Advisory (CSA) to warn of offensive capabilities developed by [...] The post US gov agencies e private firms warn nation-state actors are targeting ICS & SCADA devices appeared first on Security Affairs.

Cyware News - Latest Cyber News

Wind turbine firm Nordex hit by Conti ransomware attack

The Conti ransomware operation has claimed responsibility for a cyberattack on wind turbine giant Nordex, which was forced to shut down IT systems and remote access to the managed turbines earlier this month.

Cyware News - Latest Cyber News

Google has released a Chrome update for Windows, Mac, and Linux, to fix a high-severity zero-day vulnerability, tracked as CVE-2022-1364, actively used by threat actors in attacks.

Cyware News - Latest Cyber News

Hackers target Ukrainian govt with IcedID malware, Zimbra exploits

The CERT-UA detected the new campaigns and attributed the IcedID phishing attack to the UAC-0041 threat cluster, previously connected with AgentTesla distribution, and the second to UAC-0097, a currently unknown actor.

CyberScoop

House panel launches probe of government contracts with identity verification company ID.me

The committee twice cited CyberScoop reporting on the firm. The post House panel launches probe of government contracts with identity verification company ID.me appeared first on CyberScoop.

Cyware News - Latest Cyber News

Lazarus Targets Chemical Sector

The campaign appears to be a continuation of Lazarus activity dubbed Operation Dream Job, which was first observed in August 2020. In the past, it targeted the defense, government, and engineering sectors.

IT Security Guru

Microsoft disrupts ZLoader Cybercrime Botnet

A global consortium of cybersecurity companies have collaborated with Microsoft to disrupt the Zloader botnet. The operation succeeded in seizing control of 65 domains used to control and communicate with infected hosts. "ZLoader is made up of computing devices in businesses, hospitals, schools, and homes around the world and is run by a global internet-based [...] The post Microsoft disrupts ZLoader Cybercrime Botnet appeared first on IT Security Guru.

The Hacker News

Rarible NFT Marketplace Flaw Could've Let Attackers Hijack Crypto Wallets

Cybersecurity researchers have disclosed a now-fixed security flaw in the Rarible non-fungible token (NFT) marketplace that, if successfully exploited, could have led to account takeover and theft of cryptocurrency assets. "By luring victims to click on a malicious NFT, an attacker can take full control of the victim's crypto wallet to steal funds," Check Point researchers Roman Zaikin, Dikla

Cyware News - Latest Cyber News

Several Vulnerabilities Allow Disabling of Palo Alto Networks Products

The researcher discovered that the agent can be disabled by a local attacker with administrator privileges simply by modifying a registry key, leaving the endpoint exposed to attacks.

Cyware News - Latest Cyber News

U.S. ties North Korean hacker group to Axie Infinity crypto theft

The United States has linked the North Korean hackers to the theft of hundreds of millions of dollars' worth of cryptocurrency tied to the popular online game Axie Infinity.

Security Affairs

Ways to Develop a Cybersecurity Training Program for Employees

Cybersecurity experts would have you believe that your organization's employees have a crucial role in bolstering or damaging your company's security initiatives. While you may disagree, data breach studies show that employees and negligence are the most typical causes of security breaches, yet these prevalent issues are least discussed. According to a recent industry report [...] The post Ways to Develop a Cybersecurity Training Program for Employees appeared first on Security Affairs.

Twitter

huntr Hacktivity

Out-of-bounds Read in (CVE-2022-1296) reported by hmsec - Patch: #bugbounty #infosec #opensource

huntr Hacktivity

Out-of-bounds Read in (CVE-2022-1297) reported by hmsec - Patch: #bugbounty #infosec #opensource

Open Source CVEs

(CVE-2022-1297): Out-of-bounds Read in radareorg/radare2. Disclosed by , fixed by @trufae... #opensource #CVE #bugbounty #security #vulnerability

Remotely Alerts

Severity: | The Block Bad Bots and Stop Bad Bots Cra... | CVE-2022-0949 | Link for more:

Threat Intel Center

NEW: CVE-2022-0949 The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 6.930 does not properly sanitise and escape the fingerprint parameter before using ... (click for more) Severity: CRITICAL

vulnonym

I declare CVE-2022-0949 to be named Quizzical Genetta

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2022-0949 The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 6.930 does no... CVSS: 9.15 #Stopbadbots #CVE #CyberSecurity

Lesley Carhart

@TheBlondeRN @BlueLightsShine Joining the military at 17 turned my life around. I went from a screw up teen to having three degrees, making SNCO, becoming a leading cybersecurity expert and Director, getting two black belts, and mentoring kids.

Open Source CVEs

(CVE-2022-1296): Out-of-bounds Read in radareorg/radare2. Disclosed by , fixed by @trufae... #opensource #CVE #bugbounty #security #vulnerability

Threat Intel Center

NEW: CVE-2022-0949 The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 6.930 does not properly sanitise and escape the fingerprint parameter before using ... (click for more) Severity: CRITICAL

Linagora #infosec

Wordpress - CVE-2022-0949:

Vulmon Vulnerability Feed

CVE-2022-0949 The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 6.930 does not properly sanitise and escape the fingerprint parameter before using it in a S...

CVE

CVE-2022-0949 The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 6.930 does not properly sanitise and escape the fingerprint parameter before using it in a SQL statement via the stopbadbots_g...

Source: NIST

NIST CVE: Critical

CVE-2022-27477

Newbee-Mall v1.0.0 was discovered to contain an arbitrary file upload via the Upload function at /admin/goods/edit.

CRITICAL Vector: network Created: 2022-04-10 Updated: 2022-04-15

CVE-2022-1297

Out-of-bounds Read in r_bin_ne_get_entrypoints function in **GitHub** repository radareorg/radare2 prior to 5.6.8. This vulnerability may allow attackers to read sensitive information or cause a crash.

CRITICAL Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-1296

Out-of-bounds read in `r_bin_ne_get_relocs` function in **GitHub** repository radareorg/radare2 prior to 5.6.8. This vulnerability may allow attackers to read sensitive information or cause a crash.

CRITICAL Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-0949

The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection **WordPress** plugin before 6.930 does not properly sanitise and escape the fingerprint parameter before using it in a SQL statement via the stopbadbots_grava_fingerprint AJAX action, available to unauthenticated users, leading to a SQL injection

CRITICAL Vector: network Created: 2022-04-11 Updated: 2022-04-15

Source: NIST

NIST CVE: High

CVE-2022-26413

A command injection vulnerability in the CGI program of **Zyxel** VMG3312-T20A firmware version 5.30(ABFX.5)C0 could allow a local authenticated attacker to execute arbitrary OS commands on a vulnerable device via a LAN interface.

HIGH Vector: adjacent_network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-32156

A cross-site request forgery (CSRF) vulnerability exists in **Webmin** 1.973 via the Scheduled Cron Jobs feature.

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-0556

A local privilege escalation vulnerability caused by incorrect permission assignment in some directories of the **Zyxel** AP **Configurator** (ZAC) version 1.1.4, which could allow an attacker to execute arbitrary code as a local administrator.

HIGH Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-1252

Exposure of Private Personal Information to an Unauthorized Actor in **GitHub** repository gnuboard/gnuboard5 prior to and including 5.5.5. A vulnerability in gnuboard v5.5.5 and below uses weak encryption algorithms leading to sensitive information exposure. This allows an attacker to derive the email address of any user, including when the 'Let others see my information.' box is ticked off.

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-32162

A Cross-site request forgery (CSRF) vulnerability exists in **Webmin** 1.973 through the File Manager feature.

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-32159

A Cross-site request forgery (CSRF) vulnerability exists in **Webmin** 1.973 via the Upload and Download feature.

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-27041

Due to lack of protection, parameter student_id in **OpenSIS** Classic 8.0 /modules/eligibility/Student.php can be used to inject SQL queries to extract information from databases.

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-27089

In **Fujitsu** PlugFree Network <= 7.3.0.3, an Unquoted service path in PFNService.exe software allows a local attacker to potentially escalate privileges to system level.

HIGH Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-27088

Ivanti DSM Remote <= 6.3.1.1862 is vulnerable to an unquoted service path allowing local users to launch processes with elevated privileges.

HIGH Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-1023

The Podcast Importer SecondLine **WordPress** plugin before 1.3.8 does not sanitise and properly escape some imported data, which could allow SQL injection attacks to be performed by imported a malicious podcast file

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-1008

The One Click Demo Import **WordPress** plugin before 3.1.0 does not validate the imported file, allowing high privilege users such as admin to upload arbitrary files (such as PHP) even when FILE_MODS and FILE_EDIT are disallowed

HIGH Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-28893

The SUNRPC subsystem in the **Linux** kernel through 5.17.2 can call xs_xprt_free before ensuring that sockets are in the intended state.

HIGH Vector: local Created: 2022-04-11 Updated: 2022-04-15

Source: NIST

NIST CVE: Medium

CVE-2021-32160

A Cross-Site Scripting (XSS) vulnerability exists in **Webmin** 1.973 through the Add Users feature.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-32158

A Cross-Site Scripting (XSS) vulnerability exists in **Webmin** 1.973 via the Upload and Download feature.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-36846

Authenticated (admin or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Premio Chaty (WordPress plugin) <= 2.8.3

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-39068

IBM Curam Social Program Management 8.0.1 and 7.0.11 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 215306.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-20064

In ccci, there is a possible leak of kernel pointer due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108617; Issue ID: ALPS06108617.

MEDIUM Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-20062

In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS05836418; Issue ID: ALPS05836418.

MEDIUM Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-27958

Insecure permissions configured in the userid parameter at /user/getuserprofile of FEBS-Security v1.0 allows attackers to access and arbitrarily modify users' personal information.

MEDIUM Vector: network Created: 2022-04-10 Updated: 2022-04-15

CVE-2022-1045

Stored XSS viva .svg file upload in **GitHub** repository polonel/trudesk prior to v1.2.0.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2021-32161

A Cross-Site Scripting (XSS) vulnerability exists in **Webmin** 1.973 through the File Manager feature.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-26414

A potential buffer overflow vulnerability was identified in some internal functions of **Zyxel** VMG3312-T20A firmware version 5.30(ABFX.5)C0, which could be exploited by a local authenticated attacker to cause a denial of service.

MEDIUM Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-27156

Daylight **Studio Fuel CMS** 1.5.1 is vulnerable to HTML Injection.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-20063

In atf (spm), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06171715; Issue ID: ALPS06171715.

MEDIUM Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-20052

In mdp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS05836642; Issue ID: ALPS05836642.

MEDIUM Vector: local Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-27960

Insecure permissions configured in the user_id parameter at SysUserController.java of **OFCMS** v1.1.4 allows attackers to access and arbitrarily modify users' personal information.

MEDIUM Vector: network Created: 2022-04-10 Updated: 2022-04-15

CVE-2022-27111

Jfinal_CMS 5.1.0 allows attackers to use the feedback function to send malicious XSS code to the administrator backend and execute it.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

CVE-2022-0969

The Image optimization & Lazy Load by Optimole **WordPress** plugin before 3.3.2 does not sanitise and escape its "Lazyload background images for selectors" settings, which could allow high privilege users such as admin to perform Cross-Site scripting attacks even when the unfiltered_html capability is disallowed.

MEDIUM Vector: network Created: 2022-04-11 Updated: 2022-04-15

Source: NIST

NIST CVE: Unrated

CVE-2022-27480

A vulnerability has been identified in **SICAM A8000** CP-8031 (All versions < V4.80), **SICAM A8000 CP-8050** (All versions < V4.80). Affected devices do not require an user to be authenticated to access certain files. This could allow unauthenticated attackers to download these files.

UNRATED Vector: unkown Created: 2022-04-12 Updated: 2022-04-15

CVE-2022-26651

An issue was discovered in **Asterisk** through 19.x and **Certified Asterisk** through 16.8-cert13. The func_odbc module provides possibly inadequate escaping functionality for backslash characters in SQL queries, resulting in user-provided data creating a broken SQL query or possibly a SQL injection. This is fixed in 16.25.2, 18.11.2, and 19.3.2, and 16.8-cert14.

UNRATED Vector: Created: 2022-04- Updated: 2022-04-

CVE-2022-26498

An issue was discovered in **Asterisk** through 19.x. When using STIR/SHAKEN, it is possible to download files that are not certificates. These files could be much larger than what one would expect to download, leading to Resource Exhaustion. This is fixed in 16.25.2, 18.11.2, and 19.3.2.

UNRATED Vector: unkown Created: 2022-04-15 Updated: 2022-04-15

CVE-2022-1328

Buffer Overflow in uudecoder in **Mutt** affecting all versions starting from 0.94.13 before 2.2.3 allows read past end of input line

UNRATED Vector: unkown Created: 2022-04-14 Updated: 2022-04-15

CVE-2021-40386

Kaseya Unitrends Client/Agent through 10.5,5 allows remote attackers to execute arbitrary code.

UNRATED Vector: unkown Created: 2022-04-15 Updated: 2022-04-15

CVE-2022-28345

The **Signal** app before 5.34 for iOS allows URI spoofing via RTLO injection. It incorrectly renders RTLO encoded URLs beginning with a non-breaking space, when there is a hash character in the URL. This technique allows a remote unauthenticated attacker to send legitimate looking links, appearing to be any website URL, by abusing the non-http/non-https automatic rendering of URLs. An attacker can spoof, for example, example.com, and masquerade any URL with a malicious destination. An attacker requires a subdomain such as gepj, txt, fdp, or xcod, which would appear backwards as jpeg, txt, pdf, and docx respectively.

UNRATED Vector: unkown Created: 2022-04-15 Updated: 2022-04-15

unkown 15 15

CVE-2022-26499

An SSRF issue was discovered in **Asterisk** through 19.x. When using STIR/SHAKEN, it's possible to send arbitrary requests (such as GET) to interfaces such as localhost by using the Identity header. This is fixed in 16.25.2, 18.11.2, and 19.3.2.

UNRATED Vector: unkown Created: 2022-04-15 Updated: 2022-04-15

CVE-2022-26034

Improper authentication vulnerability in the communication protocol provided by AD (Automation Design) server of **CENTUM VP** R6.01.10 to R6.09.00, CENTUM VP Small R6.01.10 to R6.09.00, CENTUM VP Basic R6.01.10 to R6.09.00, and B/M9000 VP R8.01.01 to R8.03.01 allows an attacker to use the functions provided by AD server. This may lead to leakage or tampering of data managed by AD server.

UNRATED Vector: unkown Created: 2022-04-15 Updated: 2022-04-15

CVE-2022-27188

OS command injection vulnerability exists in **CENTUM VP** R4.01.00 to R4.03.00, CENTUM VP Small R4.01.00 to R4.03.00, CENTUM VP Basic R4.01.00 to R4.03.00, and B/M9000 VP R6.01.01 to R6.03.02, which may allow an attacker who can access the computer where the affected product is installed to execute an arbitrary OS command by altering a file generated using Graphic Builder.

UNRATED Vector: unkown Created: 2022-04-15 Updated: 2022-04-15

Source: Hybrid Analysis

Top malicious files

100% Threat score	41abddf3a8195c6f0cdef335b95d2404331b39520c917a36cfa054cef9a8dfe8.xls
100% Threat score	NBS_CertHelper.exe
100% Threat score	MoaSignEXSetup.exe
100% Threat score	ÐœÐ¾Ð±Ñ–Ð»Ñ–Ð·Ð°Ñ†Ñ–Ð¹Ð½Ð¸Ð¹ ÑÐ¿Ð¸ÑÐ¾Ðº.xls
100% Threat score	445
100% Threat score	1
86% Threat score	tmprcrlq2k_
80% Threat score	QR__Barcode_Scanner_v3.1.0__Pro__UserUpload.Net.apk
80% Threat score	RFQ - Request for Quotation.exe
75% Threat score	rssguard-4.2.1-74e3fd65-win64.exe

100% Threat score	tmp52mr15v7
100% Threat score	334.msi
100% Threat score	ê¸°í”„íŠ¸ì¹´ë“œ ìƒì„±ê¸° v2.exe
100% Threat score	WebLaunchRecorder.exe
100% Threat score	1646265799-11b7877eb4686720001-TybRpD_part_001.xlsm
91% Threat score	ddos_toolv2.exe
81% Threat score	CCleaner_v6.3.0_MOD_apkmody.io.apk
80% Threat score	INISAFEMoaSignEX.exe
77% Threat score	tmpo9ji3vk3
75% Threat score	tmpqtsx0e5s

Source: Hybrid Analysis

Top malicious URL

93% Threat score	http://112.31.211.236:54967/Mozi.m
91% Threat score	http://117.208.140.115:44256/Mozi.m

93% Threat score	http://117.213.44.89:34100/Mozi.m
91% Threat score	http://125.41.231.1:53896/Mozi.m

91%
Threat score

http://42,235,40,22:34690/Mozi,m

91%
Threat score

http://120,138,4,4:57694/Mozi,m

75%
Threat score

http://url8585,cch,com/ls/click?upn=FChruKPivNdOAyUK5pTmFeYTaligAvErF8KxPTdy-2FmT8otRAplZgy22l8TBfe4uZKTBn17rXQzMJh2LGOn4qO1py8JdeISo2PiKKWhz-2B8tNXlI3n2R-2FUemK1HCz-2B2E792bixYxCBWWeQcXbW-2B-2Bvu5NQUD7LIoqZ2hoAR-2FScM2x0cAAJHxLYiyyLTmOzUpxkoIm8aWwBRv43woTX1Rnsq0Z-2BVjBDV4r0mvyVL6ljmqknacQoyogukwqfz9vPRixBIQNDyqal5iAK-2BSONXzbzKhw-3D-3DiJvu_r6iuCa5MxmtF6lUKk019hQFy6AfIRWowNF9rKe5Ao6289bSrVFkc0sfs3G1Nb2uKzka-2FYJV0B5ng9K0HQ4A045nODI-2FAG27VW3j4BEt4mphnb2SrzA2I3D2CsTkX8Xt6TLk2WuvhSY27SkQiElLyv1BbIwOFE8z4nXC15T3topQfBA98O3-2FHt9SuX8UPlcGGbJ1cs1tVAZhceFkMXw9bEbHzds8b0vN2ixB-2F71GAy4s-3D

73%
Threat score

http://automattic,com/

Source: SpamHaus

Top spamming countries

#1 United States of America

#2 China

#3 Russian Federation

#4 Mexico

#5 Dominican Republic

#6 Saudi Arabia

#7 Uruguay

#8 India

#9 Brazil

#10 Japan

Source: SpamHaus

Top spammers

#1 **Canadian Pharmacy**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.

#2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.

#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

#4 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#5 **RetroCubes**
Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

#6 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.

#7 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#8 **Kobeni Solutions**
High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.

#9 **Richpro Trade Inc. / Richvestor GmbH**
Uses botnets or hires botnet spammers to send spam linking back to suspect investment, "quack-health-cures" and other sites that he owns or is an affiliate of. Botnet spamming and hosting sites on hacked servers is fully criminal in much of the world. Managed or owned by a Timo Richert.

Source: SpamHaus

Top countries with botnet

#1 China

#2 India

#3 United States of America

#4 Indonesia

#5 Thailand

#6 Viet Nam

#7 Algeria

#8 Brazil

#9 Pakistan

#10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

#1 United States

#2 Germany

#3 Japan

#4 Netherlands

#5 Russia

#6 India

#7 France

#8 Hong Kong

#9 Singapore

#10 United Kingdom

Source: Have I been pwned?

Have I been pwnd

Avvo (avvo.com)
In approximately December 2019, an alleged data breach of the lawyer directory service Avvo was published to an online hacking forum and used in an extortion scam (it's possible the exposure dates back earlier than that). The data contained 4.1M unique email addresses alongside SHA-1 hashes, most likely representing user passwords. Multiple attempts at contacting Avvo over the course of a week were unsuccessful and the authenticity of the data was eventually verified with common Avvo and HIBP subscribers.

Count: 4101101 Created: 2019-12-17 Updated: 2022-04-15

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets

Source: Ransom Watch

Ransomware attacks

conti	CJ Pony Parts	alphv	eNoah it solutions
lockbit2	museum-dingo	midas	Basra Multipurposr Terminal
conti	Big Horn Plastering of Colorado, Inc,	lockbit2	cassinobuilding,,,
lockbit2	cyberapex,com	suncrypt	Gemeente Buren
lockbit2	kpcg,com,hk	lockbit2	mpm,fr
lorenz	Musco Sports Lighting	lockbit2	radmangroup,com
lockbit2	soharportandfre,,,	lockbit2	verifiedlabel,c,,,