Your Security Rabbits report for March 31, 2022

Hot topics

Nothing today

Source: Ransom Watch

Ransomware attacks

stormous	infotech ua
snatch	Yip in Tsoi
blackbyte	Autumn Transport
lockbit2	botswana
lockbit2	grupodeincendio,,,
lockbit2	jlmsolicitors,c,,,
lockbit2	papierswhitebi
pandora	United Cumberland
lockbit2	omalleytunstall,,,
conti	Zeeland Farm Services, Inc,
lockbit2	avcimmedia,com
lockbit2	burlingtonsafet,,,
pandora	Hearst
blackbyte	London College of Beauty Therapy
conti	Scott Manufacturing, LLC

Source: NIST

NIST CVE: Critical

CVE-2022-22274

A Stack-based buffer overflow vulnerability in the **SonicOS** via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the **firewall**.

CRITICAL Vector: network Created: 2022-03-25 Updated: 2022-03-31

CVE-2022-26198

Notable v1.8.4 does not filter text editing, allowing attackers to execute arbitrary code via a crafted payload injected into the Title text field.

CRITICAL Vector: network Created: 2022-03-27 Updated: 2022-03-31

CVE-2022-25577

ALF-BanCO v8.2.5 and below was discovered to use a hardcoded password to encrypt the **SQLite** database containing the user's data. Attackers who are able to gain remote or local access to the system are able to read and modify the data.

CRITICAL Vector: network Created: 2022-03-25 Updated: 2022-03-31

CVE-2022-22995

The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code.

CRITICAL Vector: network Created: 2022-03-25 Updated: 2022-03-31

News

Naked Security

"VMware Spring Cloud" Java bug gives instant remote code execution - update now!
Easy unauthenticated remote code execution - PoC code already out

Security Affairs

A critical RCE vulnerability affects SonicWall Firewall appliances
SonicWall released security updates to address a remote code execution vulnerability that affects multiple firewall appliances. SonicWall has released security updates to address a critical vulnerability (CVE-2022-22274) that impacts multiple firewall appliances that could be exploited by an unauthenticated, remote attacker to execute arbitrary code and trigger a denial-of-service (DoS) condition. The CVE-2022-22274 is a [...] The post A critical RCE vulnerability affects SonicWall Firewall appliances appeared first on Security Affairs.

Cyware News - Latest Cyber News

A Third of UK Businesses Experience Cyber-Attacks at Least Once a Week
Around a third (31%) of businesses experience cyber-attacks or breaches at least once a week, according to new figures published in the UK government's Cyber Security Breaches Survey 2022 report.

Security Affairs

Bad OPSEC allowed researchers to uncover Mars stealer operation
The Morphisec Labs researchers analyzed a new malware, tracked as Mars stealer, which is based on the older Oski Stealer. Morphisec Labs recently discovered the Mars stealer that was spreading masqueraded as malicious software cracks and keygens. The Mars stealer is available for sale on several underground forums, researchers pointed out that it is under constant [...] The post Bad OPSEC allowed researchers to uncover Mars stealer operation appeared first on Security Affairs.

IT Security Guru

820,000 NYC students have their personal data exposed
Hackers breached the IT systems of Illuminate Education in January, gaining access to the personal data of around 820,000 current and former New York City public school students. Illuminate Education is a taxpayer funded software based in California. It is best known for creating the widely-used IO classroom,Skedula and PupilPath platforms, current used by New York City's [...] The post 820,000 NYC students have their personal data exposed appeared first on IT Security Guru.

IT Security Guru

A third of malware infections use Log4Shell
Researchers at Lacework have revealed that the Log4Shell vulnerability was exploited as an initial attack vector in 31% of cases monitored by the company over the past six months. The software vendor's latest Lacework Cloud Threat Report highlights typical risks in today's digital landscape. The findings confirm what security experts suspected, that the Log4j bug was used [...] The post A third of malware infections use Log4Shell appeared first on IT Security Guru.

ZDNet | security RSS

As Lapsus$ comes back from 'vacation,' Sitel clarifies position on data breach
Lapsus$ also claims to have compromised a software solutions provider.

Cyware News - Latest Cyber News

Chrome Browser Gets Major Security Update
Google this week released a security-themed Chrome 100.0.4896.60 browser makeover with patches for 28 documented vulnerabilities, some serious enough to lead to code execution attacks.

Security Affairs

CISA and DoE warns of attacks targeting UPS devices

The US CISA and the Department of Energy issued guidance on mitigating attacks against uninterruptible power supply (UPS) devices. The US Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy published joint guidance on mitigating cyber attacks against uninterruptible power supply (UPS) devices. The US agencies warn of threat actors gaining access to […] The post CISA and DoE warns of attacks targeting UPS devices appeared first on Security Affairs.

Cyware News - Latest Cyber News

Conti Continues To Attack Even After Recent Code Leaks

Researchers have spotted an updated version of Conti ransomware as part of the global ransomware tracking efforts that allow it to reboot and encrypt the targeted system in Safe Mode. To avoid detection, Conti uses the Murmur3 hashing algorithm, which produces different hash values for all API functions used, which helps avoid security software that searches for the related hash values.

Threatpost

Cyberattackers Target UPS Backup Power Devices in Mission-Critical Environments

The active attacks could result in critical-infrastructure damage, business disruption, lateral movement and more.

CyberScoop

FBI arrests 65 in BEC scams that took $51M from US businesses

"Operation Eagle Sweep" is the latest crackdown on business email compromise (BEC) scams by international law enforcement. The post FBI arrests 65 in BEC scams that took $51M from US businesses appeared first on CyberScoop.

ZDNet | security RSS

Globant admits to data breach after Lapsus$ releases source code

The hacking group criticized Globant's "poor security practices."

The Hacker News

Honda's Keyless Access Bug Could Let Thieves Remotely Unlock and Start Vehicles

A duo of researchers has released a proof-of-concept (PoC) demonstrating the ability for a malicious actor to remote lock, unlock, and even start Honda and Acura vehicles by means of what's called a replay attack. The attack is made possible, thanks to a vulnerability in its remote keyless system (CVE-2022-27254) that affects Honda Civic LX, EX, EX-L, Touring, Si, and Type R models manufactured

The Hacker News

IT Firm Globant Confirms Breach after LAPSUS$ Leaks 70GB of Data

The LAPSUS$ data extortion gang announced their return on Telegram after a week-long "vacation," leaking what they claim is data from software services company Globant. "We are officially back from a vacation," the group wrote on their Telegram channel - which has nearly around 54,000 members as of writing - posting images of extracted data and credentials belonging to the company's DevOps

Security Affairs

Lapsus$ extortion gang claims to have hacked IT Giant Globant

The Lapsus$ extortion group claims to have hacked IT giant Globant and leaked tens of gigabytes of stolen data. The Lapsus$ extortion group claims to have hacked IT giant Globant and leaked roughly 70 Gb of stolen data. The gang claims that the company has implemented poor security practices that allowed them to hack their […] The post Lapsus$ extortion gang claims to have hacked IT Giant Globant appeared first on Security Affairs.

Cyware News - Latest Cyber News

Mazda Infotainment Crash Shows How Fragile Car Security Really Is

The complete details of the coding error that led to the crash of Mazda CMUs weren't published, but experts believe that it was caused due to a type of NULL dereference vulnerability.

Cyware News - Latest Cyber News

Muhstik Botnet Gang Targets Redis Exploit Within One Day of Public POC Release

Muhstik botnet operators were found exploiting a recently disclosed bug in some Redis Debian packages to infiltrate servers and then use it for DDOS attacks. The attackers target the vulnerability CVE-2022-0543 in Redis Debian packages. To protect against this particular attack, users are recommended to update their packages to Redis package version 5.6.0.16.-1 or follow the Debian security advisory or Ubuntu's security bulletin on the issue.

IT Security Guru

NCSC suggests rethinking Russian supply chain risks

The National Cyber Security Centre (NCSC) of the UK has urged organisations to reconsider the risks associated with "Russian-controlled" parts of their supply chains. Ian Levy, technical director of the NCSC argued that "Russian law already contains legal obligations on companies to assist the Russian Federal Security Service (FSB), and the pressure to do so […] The post NCSC suggests rethinking Russian supply chain risks appeared first on IT Security Guru.

The Hacker News

QNAP Warns of OpenSSL Infinite Loop Vulnerability Affecting NAS Devices

Taiwanese company QNAP this week revealed that a selected number of its network-attached storage (NAS) appliances are affected by a recently-disclosed bug in the open-source OpenSSL cryptographic library. "An infinite loop vulnerability in OpenSSL has been reported to affect certain QNAP NAS," the company said in an advisory published on March 29, 2022. "If exploited, the vulnerability allows

Remcos Trojan: Analyzing the Attack Chain

This infection contains many stages and largely depends on the C2 server, which stores the required files for each stage. The attacker also uses a

Cyware News - Latest Cyber News

Cloaked Snags $25M Funding to Tackle Data-Sharing Privacy

The startup, called Cloaked, said the Series A investment was co-led by Lux Capital and Human Capital and will be used to exit beta and drive growth in a competitive marketplace.

Cyware News - Latest Cyber News

Crypto Stealing Malware Spreads via Fake Wallet Apps

Researchers found dozens of trojanized cryptocurrency wallet apps attempting to steal cryptocurrency funds, especially from Chinese users. ESET researchers have revealed over 40 copycat websites of popular cryptocurrency wallets. Smartphone users are suggested to stay vigilant and use genuine mobile wallets and exchange apps downloaded from official app stores explicitly associated with their official websites.

Cyware News - Latest Cyber News

Cyera Launches From Stealth With $60M to Identify, Secure, and Remediate Cloud Data Security Risks

Cyera launched from stealth with $60 million in funding, which comes just ten months after Cyera's formation. The financing was led by Sequoia Capital, alongside Accel, and Cyberstarts.

Cyware News - Latest Cyber News

French National Health Insurance Fund Suffers Massive Data Leak

Data stolen from affected members of the French health insurance body included names, surnames, date of birth, social security numbers, GP details, and levels of reimbursement.

Threatpost

Google Chrome Bug Actively Exploited as Zero-Day

The internet giant issued an update for the bug, which is found in the open-source V8 JavaScript engine.

The Hacker News

Improve Your Hacking Skills with 9 Python Courses for Just $39

For anyone with interest in cybersecurity, learning Python is a must. The language is used extensively in white hat hacking, and professionals use Python scripts to automate tests. It also has a use in the "soft" side of cybersecurity -- like scraping the web for compromised data and detecting bugs. Featuring nine full-length video courses, The Complete 2022 Python Programmer Bundle helps you

Threatpost

Lapsus$ 'Back from Vacation'

Lapsus$ added IT giant Globant plus 70GB of leaked data - including admin credentials for scads of customers' DevOps platforms - to its hit list.

Cyware News - Latest Cyber News

Log4Shell Used in a Third of Malware Infections

The infamous Log4Shell vulnerability was exploited as an initial infection vector in 31% of cases monitored by Lacework over the past six months, highlighting risks present in today's digital supply chain.

Threatpost

MSHTML Flaw Exploited to Attack Russian Dissidents

A Ukrainian-based threat actor is spearphishing Russians who are using services that have been banned by the Kremlin.

Security Affairs

Mysterious disclosure of a zero-day RCE flaw Spring4Shell in Spring

An unauthenticated zero-day RCE vulnerability in the Spring Core Java framework called 'Spring4Shell' has been publicly disclosed. Researchers disclosed a zero-day vulnerability, dubbed Spring4Shell, in the Spring Core Java framework called 'Spring4Shell.' An unauthenticated, remote attacker could trigger the vulnerability to execute arbitrary code on the target system. The framework is currently maintained by Spring.io […] The post Mysterious disclosure of a zero-day RCE flaw Spring4Shell in Spring appeared first on Security Affairs.

IT Security Guru

NHS 111 urgent care provider leads the way in secure and flexible workforce identity and access management with My1Login

My1Login has announced it has been hired by London Central & West Unscheduled Care Collaborative, a leading provider of urgent healthcare to the NHS 111 service, to overhaul its staff identity access through My1Login's Identity-as-a-Service (IDaaS) solution. The platform integrates with their existing computer login and removes the need for users to manage any […] The post NHS 111 urgent care provider leads the way in secure and flexible workforce identity and access management with My1Login appeared first on IT Security Guru.

Threatpost

RCE Bug in Spring Cloud Could Be the Next Log4Shell, Researchers Warn

The so-called 'Spring4Shell' bug has cropped up, so to speak, and could be lurking in any number of Java applications.

The Hacker

Researchers Expose Mars Stealer Malware Campaign Using Google Ads to Spread

A nascent information stealer called Mars has been observed in campaigns that

Cyware News - Latest Cyber News

password-protected .xls file to lower the detection rate.

IT Security Guru

Ronin blockchain hit with $620 million crypto heist
Sky Mavis' Ronin Network, which supports its Axie Infinity game, has suffered the largest cryptocurrency theft in history. The organisation announced yesterday that the Ronin network had been hacked to the tune of 173,000 Ethereum, or roughly $594 million, and $25 million in US dollars. Comparitech has ranked the incident as the largest crypto-heist of […] The post Ronin blockchain hit with $620 million crypto heist appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Singapore, US to establish dialogue to strengthen cooperation in cybersecurity
The United States-Singapore Cyber Dialogue, as it is called, will bring together senior government officials from the cyber operational, technical, and policy units of various agencies on both sides.

ZDNet | security RSS

This new ransomware targets data visualization tool Jupyter Notebook
Misconfigured environments are the entry point for the ransomware strain.

IT Security Guru

Unpatched SpringShell bug threatens web app security
A new critical remote code execution bug, dubbed "SpringShell" by some in the community, has been identified by security researchers. The vulnerability impacts the spring-core artifact, a popular framework used extensively in Java applications, specifically with JKD9 or newer. Sonatype explained, "the vulnerability affects anyone using spring-core, a core part of the Spring Framework, to […] The post Unpatched SpringShell bug threatens web app security appeared first on IT Security Guru.

CyberScoop

US telecommunications company likely targeted by Russian hackers shares details of Feb. 24 attack
New details suggest the incident was less complicated than initially thought, even as the attacks continue. The post US telecommunications company likely targeted by Russian hackers shares details of Feb. 24 attack appeared first on CyberScoop.

WeLiveSecurity

Women in tech: Unique insights from a lifelong pursuit of innovation
Leading Slovak computer scientist Maria Bielikova shares her experience working as a woman driving technological innovation and reflects on how to inspire the next generation of talent in tech The post Women in tech: Unique insights from a lifelong pursuit of innovation appeared first on WeLiveSecurity

News

take advantage of cracked versions of the malware to steal information stored in web browsers and cryptocurrency wallets. "Mars Stealer is being distributed via social engineering techniques, malspam campaigns, malicious software cracks, and keygens," Morphisec malware researcher Arnold Osipov said in a report

CyberScoop

Russian, Chinese, Belarusian hackers increasingly using Ukraine-themed lures in attacks, Google observes
The Threat Analysis Group report sheds light on international efforts to leverage the war in hacking campaigns. The post Russian, Chinese, Belarusian hackers increasingly using Ukraine-themed lures in attacks, Google observes appeared first on CyberScoop.

Cyware News - Latest Cyber News

SQL injection protections in ImpressCMS could be bypassed to achieve RCE
Vulnerabilities in ImpressCMS could allow an unauthenticated attacker to bypass the software's SQL injection protections to achieve remote code execution (RCE), a security researcher has warned.

The Hacker News

Unpatched Java Spring Framework 0-Day RCE Bug Threatens Enterprise Web Apps Security
A zero-day remote code execution (RCE) vulnerability has come to light in the Spring framework shortly after a Chinese security researcher briefly leaked a proof-of-concept (PoC) exploit on GitHub before deleting their account. According to cybersecurity firm Praetorian, the unpatched flaw impacts Spring Core on Java Development Kit (JDK) versions 9 and later and is a bypass for another

Cyware News - Latest Cyber News

Update: Viasat shares details on KA-SAT satellite service cyberattack
US satellite communications provider Viasat has shared an incident report regarding the cyberattack that affected its KA-SAT consumer-oriented satellite broadband service on February 24, the day Russia invaded Ukraine.

Blog â€“ Flashpoint

What Is SpringShell? What We Know About the SpringShell Vulnerability
Flashpoint and Risk Based Security have analyzed a new remote code execution (RCE) vulnerability looming in the background, dubbed "SpringShell," which could affect a wide variety of software. In some circles, SpringShell is being hyped and rumored to be as impactful as Log4Shell. But we are still collecting facts and will continuously update this blog […] The post What Is SpringShell? What We Know About the SpringShell Vulnerability appeared first on Flashpoint.

Naked Security

World Backup Day: 5 data recovery tips for everyone!
The only backup you will ever regret is the one you didn't make

Twitter

Rep. Val Demings

Last night we passed the federal budget to keep us SAFE. I voted to strengthen Americas military and provide strong resources for: - Securing our border - Homeland security grants that protect communities & houses of worship - Cybersecurity - Coast Guard and port security

Gary Gensler

Join us in now at our Investor Advisory Committee Meeting. Todays agenda includes a panel on artificial intelligence and robo-advising and a discussion on cybersecurity disclosures.

Dave Rubin

This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[…]

Spiros Margaris

The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (27%)

Russia (20%)

Germany (12%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (47%)

Ukraine (17%)

United States (17%)

Source: Imperva DDOS Map

Top DDOS techniques

67% **DDoS**

23% **Automated Threat**

10% **OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

54% **Financial Services**

22% **Business**

8% **Computing & IT**

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://gis,cat/espelta/cddjjd/?i=1
92% Threat score	http://5092312,ru/
91% Threat score	http://192,72,17,236:57566/Mozi,m
87% Threat score	http://tracking,mcargo,biz/lists/oz271ej2mh9b4/unsubscribe/bc948rd58ga09/ms342t0tmn657
82% Threat score	http://proposal,securefilesdone,workers,dev/
79% Threat score	http://r,sender,mea-finance,com/mk/mr/74sBpr1pXyGO-Bz6pHJ5_C5D-oGOT-Q-OcJRVf2FBsQ2jK8kFXu9vT4zYoscGb4IPT6m8exwddhBkIC5QC3VmhoWF2pUMvVhduScjKwGhFHqZmcNjcnCIGUVLsTvps2PV6HKhixJBg
77% Threat score	http://linktr,ee/securesharefile
74% Threat score	http://sharon,monster/
98% Threat score	http://
92% Threat score	http://
91% Threat score	http://
85% Threat score	https:/
81% Threat score	https:/
77% Threat score	http://
76% Threat score	http://www,allone,report/&dat
74% Threat score	https:/

Source: NIST

NIST CVE: High

CVE-2022-27227

In **PowerDNS Authoritative** Server before 4.4.3, 4.5.x before 4.5.4, and 4.6.x before 4.6.1 and PowerDNS **Recursor** before 4.4.8, 4.5.x before 4.5.8, and 4.6.x before 4.6.1, insufficient validation of an IXFR end condition causes incomplete zone transfers to be handled as successful transfers.

HIGH Vector: network Created: 2022-03-25 Updated: 2022-03-31

CVE-2022-27946

NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to admin_account.cgi.

HIGH Vector: network Created: 2022-03-26 Updated: 2022-03-31

CVE-2022-1071

User after free in mrb_vm_exec in **GitHub** repository mruby/mruby prior to 3.2.

HIGH Vector: local Created: 2022-03-26 Updated: 2022-03-31

CVE-2022-27947

NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the ipv6_fix.cgi ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, or ipv6_lan_length parameter.

HIGH Vector: network Created: 2022-03-26 Updated: 2022-03-31

CVE-2022-27945

NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to password.cgi.

HIGH Vector: network Created: 2022-03-26 Updated: 2022-03-31

Source: NIST

NIST CVE: Medium

CVE-2021-44768

Delta Electronics **CNCSoft** (Version 1.01.30) and prior) is vulnerable to an out-of-bounds read while processing a specific project file, which may allow an attacker to disclose information.

MEDIUM Vector: local Created: 2022-03-25 Updated: 2022-03-31

CVE-2021-46426

phpIPAM 1.4.4 allows Reflected XSS and CSRF via

CVE-2022-27943

libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

MEDIUM Vector: local Created: 2022-03-26 Updated: 2022-03-31

CVE-2022-27938

stb_image.h (aka the stb image loader) 2.19, as used in **libsixel** and app/admin/subnets/find_free_section_subnets.php of the subnets functionality.

MEDIUM Vector: network Created: 2022-03-25 Updated: 2022-03-31

other products, has a reachable assertion in stbi__create_png_image_raw.

MEDIUM Vector: local Created: 2022-03-26 Updated: 2022-03-31

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-1122

A flaw was found in the opj2_decompress program in openjpeg2 2.4.0 in the way it handles an input directory with a large number of files. When it fails to allocate a buffer to store the filenames of the input directory, it calls free() on an uninitialized pointer, leading to a segmentation fault and a denial of service.

UNRATED Vector: unkown Created: 2022-03-29 Updated: 2022-03-31

CVE-2021-45031

A vulnerability in MEPSAN's USC+ before version 3.0 has a weakness in login function which lets attackers to generate high privileged accounts passwords.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-40645

An SQL Injection vulnerability exists in glorylion JFinalOA as of 9/7/2021 in the defkey parameter getHaveDoneTaskDataList method of the FlowTaskController.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-43142

An XML External Entity (XXE) vulnerability exists in wuta jox 1.16 in the readObject method in JOXSAXBeanInput.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-27496

Cross-site scripting vulnerability in Zero-channel BBS **Plus** v0.7.4 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-25915

Improper access control vulnerability in **ELECOM** LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, **WRC-2533GST2** firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management **screen** of the product via unspecified vectors.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-24299

Improper input validation vulnerability in **pfSense** CE and pfSense **Plus** (pfSense CE software versions prior to 2.6.0 and pfSense Plus software versions prior to 22.01) allows a remote attacker with the privilege to change **OpenVPN** client or server settings to execute an arbitrary command.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2021-46006

In **Totolink** A3100R V5.9c.4577, "test.asp" contains an API-like function, which is not authenticated. Using this function, an attacker can configure multiple settings without authentication.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-46008

In **totolink** a3100r V5.9c.4577, the hard-coded telnet password can be discovered from official released firmware. An attacker, who has connected to the Wi-Fi, can easily telnet into the target with root shell if the telnet is function turned on.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-33581

MashZone NextGen through 10.7 GA has an SSRF vulnerability that allows an attacker to **interact** with arbitrary TCP services, by abusing the feature to check the availability of a PPM connection. This occurs in com.idsscheer.ppmmashup.web.webservice.impl.ZPrestoAdminWebService.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-22986

Netcommunity OG410X and OG810X series (Netcommunity OG410Xa, OG410Xi, OG810Xa, and OG810Xi firmware Ver.2.28 and earlier) allow an attacker on the adjacent network to execute an arbitrary OS command via a specially crafted config file.

CVE-2022-26645

A remote code execution (RCE) vulnerability in Online Banking System **Protect** v1.0 allows attackers to execute arbitrary code via a crafted PHP file uploaded through the Upload Image function.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2019-9564

A vulnerability in the authentication logic of Wyze Cam Pan v2, Cam v2, Cam v3 allows an attacker to bypass login and control the devices. This issue affects: Wyze Cam Pan v2 versions prior to 4.49.1.47. Wyze Cam v2 versions prior to 4.9.8.1002. Wyze Cam v3 versions prior to 4.36.8.32.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-40644

An SQL Injection vulnerability exists in oasys oa_system as of 9/7/2021 in resources/mappers/notice-mapper.xml.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-20729

Cross-site scripting vulnerability in **pfSense** CE and pfSense **Plus** (pfSense CE software versions 2.5.2 and earlier, and pfSense Plus software versions 21.05 and earlier) allows a remote attacker to inject an arbitrary script via a malicious URL.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-1160

heap buffer overflow in get_one_sourceline in **GitHub** repository vim/vim prior to 8.2.4647.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-26019

Improper access control vulnerability in **pfSense** CE and pfSense **Plus** (pfSense CE software versions prior to 2.6.0 and pfSense Plus software versions prior to 22.01) allows a remote attacker with the privilege to change NTP GPS settings to rewrite existing files on the file system, which may result in arbitrary command execution.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2021-38362

In RSA **Archer** 6.x through 6.9 SP3 (6.9.3.0), an authenticated attacker can make a GET request to a REST API endpoint that is vulnerable to an Insecure Direct Object Reference (IDOR) issue and retrieve sensitive data.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-46009

In **Totolink** A3100R V5.9c.4577, multiple pages can be read by **curl** or **Burp** Suite without authentication. Additionally, admin configurations can be set without cookies.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-33523

MashZone NextGen through 10.7 GA allows a remote authenticated user, with access to the admin console, to upload a new **JDBC** driver that can execute arbitrary commands on the underlying host. This occurs in com.idsscheer.ppmmashup.business.jdbc.DriverUploadController.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-23183

Missing authorization vulnerability in **Advanced Custom Fields** versions prior to 5.12.1 and Advanced Custom Fields Pro versions prior to 5.12.1 allows a remote authenticated attacker to view the information on the database without the access permission.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-26646

Online Banking System **Protect** v1.0 was discovered to contain a local file inclusion (LFI) vulnerability via the pages parameter.

UNRATED Vector: Created: 2022-03- Updated: 2022-03-

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-26644

Online Banking System **Protect** v1.0 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via parameters on user profile, system_info and accounts management.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-24790

Puma is a simple, fast, multi-threaded, parallel HTTP 1.1 server for Ruby/Rack applications. When using Puma behind a proxy that does not properly validate that the incoming HTTP request matches the RFC7230 standard, Puma and the frontend proxy may disagree on where a request starts and ends. This would allow requests to be smuggled via the front-end proxy to Puma. The vulnerability has been fixed in 5.6.4 and 4.3.12. Users are advised to upgrade as soon as possible. Workaround: when deploying a proxy in front of Puma, turning on any and all functionality to make sure that the request matches the RFC7230 standard.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2019-12266

Stack-based Buffer Overflow vulnerability in Wyze Cam Pan v2, Cam v2, Cam v3 allows an attacker to run arbitrary code on the affected device. This issue affects: Wyze Cam Pan v2 versions prior to 4.49.1.47. Wyze Cam v2 versions prior to 4.9.8.1002. Wyze Cam v3 versions prior to 4.36.8.32.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-46007

totolink a3100r V5.9c.4577 is vulnerable to os command injection. The backend of a page is executing the "ping" command, and the input field does not adequately filter special symbols. This can lead to command injection attacks.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-25008

totolink EX300_v2 V4.0.3c.140_B20210429 and EX1200T V4.1.2cu.5230_B20210706 does not contain an authentication mechanism.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-43664

totolink EX300_v2 V4.0.3c.140_B20210429 was discovered to contain a command injection vulnerability via the component process forceugpo.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-43662

totolink EX300_v2, ver V4.0.3c.140_B20210429 and A720R ,ver V4.1.5cu.470_B20200911 have an issue which causes uncontrolled resource consumption.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-25348

Untrusted search path vulnerability in **AttacheCase** ver.4.0.2.7 and earlier allows an attacker to gain privileges and execute arbitrary code via a Trojan horse DLL in an unspecified directory.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

unkown 30 31

CVE-2022-24763

PJSIP is a free and open source multimedia communication library written in the C language. Versions 2.12 and prior contain a denial-of-service vulnerability that affects PJSIP users that consume PJSIP's XML parsing in their apps. Users are advised to update. There are no known workarounds.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2022-1191

SSRF on index.php/cobrowse/proxycss/ in **GitHub** repository livehelperchat/livehelperchat prior to 3.96.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2021-33208

The "Register an Ehcache Configuration File" admin feature in MashZone NextGen through 10.7 GA allows XXE attacks via a malicious XML configuration file.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-46010

Totolink A3100R V5.9c.4577 suffers from Use of Insufficiently Random Values via the web configuration. The SESSION_ID is predictable. An attacker can hijack a valid session and conduct further malicious operations.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

CVE-2021-43663

totolink EX300_v2 V4.0.3c.140_B20210429 was discovered to contain a command injection vulnerability via the component cloudupdate_check.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2021-43661

totolink EX300_v2 V4.0.3c.140_B20210429 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /home.asp.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2022-28128

Untrusted search path vulnerability in **AttacheCase** ver.3.6.1.0 and earlier allows an attacker to gain privileges and execute arbitrary code via a Trojan horse DLL in an unspecified directory.

UNRATED Vector: unkown Created: 2022-03-31 Updated: 2022-03-31

CVE-2021-45900

Vivoh Webinar Manager before 3.6.3.0 has improper API authentication. When a user logs in to the administration configuration web portlet, a VIVOH_AUTH **cookie** is assigned so that they can be uniquely identified. Certain APIs can be successfully executed without proper authentication. This can let an attacker impersonate as victim and make state changing requests on their behalf.

UNRATED Vector: unkown Created: 2022-03-30 Updated: 2022-03-31

Source: SpamHaus

Top spamming countries

#1 United States of America

#2 China

#3 Russian Federation

#4 Mexico

#5 Dominican Republic

#6 Saudi Arabia

#7 India

#8 Uruguay

#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 Algeria
#7 Viet Nam
#8 Brazil
#9 Pakistan
#10 Japan

Source: SpamHaus

Top phishing countries

#1 United States
#2 Japan
#3 Germany
#4 Malaysia
#5 Russia
#6 Singapore
#7 Netherlands
#8 India
#9 South Korea
#10 Indonesia

Source: Hybrid Analysis

Top malicious files

100% Threat score	StartGame.exe	100% Threat score	tmpq66rmj1v
100% Threat score	payloadexternoNOIP.exe	100% Threat score	deme kanÄ±tÄ± Ä°ÅŸ BankasÄ±.pdf.exe
95% Threat score	3FFFA53BA11554C466D12840076F621CE9220B95903036E1199123C21FF1DCEE	85% Threat score	senza titolo 986709975.xlsm
83% Threat score	irsfoiecobfali.xls	80% Threat score	test_L.exe