



Your Security Rabbits report for March 11, 2022

Source: [Ransom Watch](#)

Ransomware attacks

Nothing today

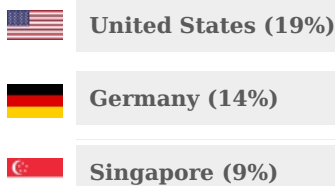
Source: [Have I been pwned?](#)

Have I been pwned

Nothing today

Source: [Imperva DDOS Map](#)

Top DDOS attackers



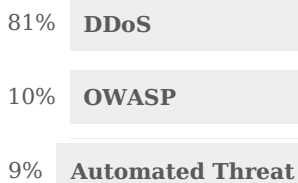
Source: [Imperva DDOS Map](#)

Top DDOS country targets



Source: [Imperva DDOS Map](#)

Top DDOS techniques



Source: [Imperva DDOS Map](#)

Top DDOS industry targets

64% **Financial Services**

27% **Business**

3% **Computing & IT**

Source: *Hybrid Analysis*

Top malicious URL

96% Threat score [http://polloniexx-aps \(.\) ml/wallet](http://polloniexx-aps (.) ml/wallet)

86% Threat score [http://88 \(.\) 119 \(.\) 170 \(.\) 124/lcekcncxkblmlwlpoklgof](http://88 (.) 119 (.) 170 (.) 124/lcekcncxkblmlwlpoklgof)

77% Threat score [http://www \(.\) akron-holding \(.\) ru/](http://www (.) akron-holding (.) ru/)

89% Threat score [http://ecowebsitedevelopment \(.\) com/includes/ecow2/ecow2/fre \(.\) php](http://ecowebsitedevelopment (.) com/includes/ecow2/ecow2/fre (.) php)

86% Threat score [http://88 \(.\) 119 \(.\) 170 \(.\) 124/ezedcjrfvjriftmldedu](http://88 (.) 119 (.) 170 (.) 124/ezedcjrfvjriftmldedu)

74% Threat score [https://ticketbud \(.\) com/events/71e2a81a-a10e-11ec-809a-42010a717019](https://ticketbud (.) com/events/71e2a81a-a10e-11ec-809a-42010a717019)

Hot topics

Nothing today

News



[A basic text-color trick can fool phishing filters](#)
Researchers at Avanan have found evidence of a phishing campaign that involves whited-out text intended to trick email security filters. The post A basic text-color trick can fool phishing filters appeared first on CyberScoop.



[Attackers Use Modified Open-Source Reverse Tunneling Utility to Gain Persistence on Infected Systems](#)
Security experts have spotted an interesting case of a suspected ransomware attack that employed custom-made tools typically used by APT (advanced persistent threat) groups.



[Brute Force and Credential Stuffing Attacks: How Cyber Threat Actors Gain Access to Accounts--Plus Best Practices for Detection and Prevention](#)
The prevalence of brute force and credential stuffing attacks Brute force and credential stuffing attacks are constant threats to organizations across the private and public sectors. Threat actors who carry out brute force and credential stuffing attacks typically do so to gain unauthorized entry to poorly secured bank, e-commerce, and other types of potentially valuable [...] The post Brute Force and Credential Stuffing Attacks: How Cyber Threat Actors Gain Access to Accounts--Plus Best Practices for Detection and Prevention appeared first on Flashpoint.



[Canadian man accused of extorting \\$28 million in ransomware scheme extradited to U.S.](#)
One of NetWalker's alleged most prolific affiliates made his first court appearance in the U.S. Thursday. The post Canadian man accused of extorting \$28 million in ransomware scheme extradited to U.S. appeared first on CyberScoop.



[CISA added 98 domains to the joint alert related to Conti ransomware gang](#)
The U.S. CISA has updated the alert on Conti ransomware and added 98 domain names used by the criminal gang. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has updated the alert on Conti ransomware operations, the agency added 100 domain names used by the group. The joint report published by CISA, the



[Conti ransomware group spent millions in 2021](#)
The prolific Conti ransomware collective spent millions on salaries, tools and services throughout 2021. The recent leak of the pro-Russia group's internal chats by a Ukrainian researcher, analysed by security vendor BreachQuest, has revealed fascinating insights into the workings of the operation. The group's structure is not dissimilar to

Federal Bureau [...] The post CISA added 98 domains to the joint alert related to Conti ransomware gang appeared first on Security Affairs.

that of a legitimate business, with [...] The post Conti ransomware group spent millions in 2021 appeared first on IT Security Guru.



Cyware
News -
Latest Cyber
News

Conti Uses New Domains After Recent Code Leaks - Warns CISA

The notoriety of the Conti ransomware group has come under the spotlight as the CISA shared an alert with IoCs consisting of close to 100 domain names. Organizations should follow mitigation strategies and recommendations provided in the alert. Besides, security admins can use provided IOCs for better detection of threats.



Cyware
News -
Latest Cyber
News

Corporate Website Contact Forms Used to Spread BazarBackdoor Malware

The stealthy information stealing BazarBackdoor malware is now being spread via website contact forms rather than typical phishing emails to evade detection by security software.



Security
Affairs

Crooks target Ukraine's IT Army with a tainted DDoS tool

Threat actors are spreading password-stealing malware disguised as a security tool to target Ukraine's IT Army. Cisco Talos researchers have uncovered a malware campaign targeting Ukraine's IT Army, threat actors are using infostealer malware mimicking a DDoS tool called the "Liberator." The Liberator tool is circulating among pro-Ukraina hackers that use it to target Russian [...] The post Crooks target Ukraine's IT Army with a tainted DDoS tool appeared first on Security Affairs.



CyberScoop

Cyber Command chief tells Congress chip shortage has national security implications

China's march toward chip independence is of "great concern" and could have "broader impacts," he said. It's an issue that dovetails with the Russia-Ukraine war. The post Cyber Command chief tells Congress chip shortage has national security implications appeared first on CyberScoop.



CyberScoop

Cybercriminals are posing as Ukraine fundraisers to steal cryptocurrency

The scams have picked up on Telegram. The post Cybercriminals are posing as Ukraine fundraisers to steal cryptocurrency appeared first on CyberScoop.



Cyware
News -
Latest Cyber
News

Exploiting a use-after-free in Windows Common Logging File System (CLFS)

Along with two other similar vulnerabilities, Microsoft patched this vulnerability in September 2021 and assigned the CVEs CVE-2021-36955, CVE-2021-36963, and CVE-2021-38633 to them.



Cyware
News -
Latest Cyber
News

HelpSystems to Acquire MDR Services Firm Alert Logic

Software firm HelpSystems continues on its cybersecurity buying spree, announcing on Wednesday that it has agreed to acquire Alert Logic, a provider of managed detection and response (MDR) services.



The Hacker
News

Iranian Hackers Targeting Turkey and Arabian Peninsula in New Malware Campaign

The Iranian state-sponsored threat actor known as MuddyWater has been attributed to a new swarm of attacks targeting Turkey and the Arabian Peninsula with the goal of deploying remote access trojans (RATs) on compromised systems. "The MuddyWater supergroup is highly motivated and can use unauthorized access to conduct espionage, intellectual property theft, and deploy ransomware and destructive



Cyware
News -
Latest Cyber
News

Iranian State-Sponsored Hackers Target Turkey and Arabian Peninsula in New SloughRAT Malware Campaign

The Iranian state-sponsored threat actor MuddyWater has been attributed to a new swarm of attacks targeting Turkey and the Arabian Peninsula with the goal of deploying RATs on compromised systems.



Security
Affairs

Lapsus\$ Ransomware Group is hiring, it announced recruitment of insiders

Lapsus\$ Ransomware gang is looking for insiders willing to sell remote access to major technology corporations and ISPs. Thursday, March 10, Lapsus\$ ransomware gang announced they're starting to recruit insiders employed within major technology giants and ISPs, such companies include Microsoft, Apple, EA Games and IBM. Their scope of interests include - major telecommunications companies [...] The post Lapsus\$ Ransomware Group is hiring, it announced recruitment of insiders appeared first on Security Affairs.



Threatpost

Malware Posing as Russia DDoS Tool Bites Pro-Ukraine Hackers

Be careful when downloading a tool to cyber-target Russia: It could be an infostealer wolf dressed in sheep's clothing that grabs your cryptocurrency info instead.



IT Security
Guru

Microsoft calls for more women in cyber

The tech giant Microsoft has claimed that encouraging women into cybersecurity jobs is "mission critical" to addressing the labour shortage in the cybersecurity industry. The company's corporate vice president of security, compliance, identity and management, Vasu Jakkal argues that diversity is sorely needed in the industry in order



to address the evolving threat landscape and [...] The post Microsoft calls for more women in cyber appeared first on IT Security Guru.



Threatpost

Most Orgs Would Take Security Bugs Over Ethical Hacking Help

A new survey suggests that security is becoming more important for enterprises, but they're still falling back on old "security by obscurity" ways.



Threatpost

Multi-Ransomware Victims Have It Coming- Podcast

Let's blame the victim. IT decision makers' confidence about security doesn't jibe with their concession that repeated incidents are their own fault, says ExtraHop's Jamie Moles.



Cyware
News -
Latest Cyber
News

Nearly 30% of critical WordPress plugin bugs don't get a patch

Patchstack, a leader in WordPress security and threat intelligence, has released a whitepaper to present the state of WordPress security in 2021, and the report paints a dire picture.



Security
Affairs

New Emotet botnet is rapidly growing, with +130K unique bots spread across 179 countries

A few months after its return the Emotet botnet has already infected over 130,000 unique bots spread across 179 countries. The Emotet botnet continues to grow and has infected approximately 130,000 hosts since its resurrection in November 2021. Early 2021, law enforcement and judicial authorities worldwide conducted a joint operation, named Operation Ladybird, which disrupted the EMOTET [...] The post New Emotet botnet is rapidly growing, with +130K unique bots spread across 179 countries appeared first on Security Affairs.



The Hacker
News

New Exploit Bypasses Existing Spectre-V2 Mitigations in Intel and Arm CPUs

Researchers have disclosed a new technique that could be used to circumvent existing hardware mitigations in modern processors from Intel, AMD, and Arm, and stage speculative execution attacks such as Spectre to leak sensitive information from host memory. Attacks like Spectre are designed to break the isolation between different applications by taking advantage of an optimization technique



CyberScoop

New security threats target industrial control and OT environments

A new Dragos report highlights recent threats targeting industrial control systems and operational technology environments and identifies strategies to address them. The post New security threats target industrial control and OT environments appeared first on CyberScoop.



Cyware
News -
Latest Cyber
News

Notorious Hacker Group Claims to Steal 200 GB of Source Code from Vodafone

The notorious hacker group, calling itself "Lapsus\$", claims to have obtained roughly 200 Gb of source code files, allegedly representing approximately 5,000 GitHub repositories.



Security
Affairs

Open database leaves major Chinese ports exposed to shipping chaos

The freight logs of two major Chinese shipping ports have been leaking data, a problem which if left unresolved could disrupt the supply chain of up to 70,000 tonnes of cargo a day, with potentially serious consequences for international shipping. The cybernews(r) research team identified an open Elasticsearch database, which contained more than 243GB of [...] The post Open database leaves major Chinese ports exposed to shipping chaos appeared first on Security Affairs.



Threatpost

Qakbot Botnet Sprouts Fangs, Injects Malware into Email Threads

The ever-shifting, ever-more-powerful malware is now hijacking email threads to download malicious DLLs that inject password-stealing code into webpages, among other foul things.



Cyware
News -
Latest Cyber
News

Qakbot injects itself into the middle of your conversations

The messages generally contain brief text content, followed by a link to download a zip archive. These links may be "bare URLs" like above, or hot-linked text in the message body.



Cyware
News -
Latest Cyber
News

Raccoon Stealer: "Trash panda" abuses Telegram

Avast researchers came across a stealer, called Raccoon Stealer, a name given to it by its author. Raccoon Stealer uses the Telegram infrastructure to store and update actual C&C addresses.



Cyware
News -
Latest Cyber
News

Researchers Discover new botnet, 'Zhadnost,' responsible for Ukraine DDoS attacks

SSC discovered a botnet of more than 3,000 unique IP addresses, across multiple countries and continents, that were the source of the DDoS attacks which consisted of HTTP floods and DNS amplification.



Cyware
News -
Latest Cyber

Russia creates its own TLS certificate authority to bypass sanctions







The sanctions imposed by western companies and governments are preventing Russian sites from renewing existing TLS certificates, causing browsers to block access to sites with expired







Threatpost

Russia May Use Ransomware Payouts to Avoid Sanctions

FinCEN warns financial institutions to beware of unusual cryptocurrency payments or illegal transactions Russia may use to evade restrictions

News	certificates.	imposed due to its invasion of Ukraine.
 Cyware News - Latest Cyber News	Russian government sites hacked in supply chain attack Websites of some Russian federal agencies were compromised in a supply chain attack on Tuesday after unknown attackers hacked the stats widget used to track the number of visitors by multiple government agencies	 The Hacker News Russian Pushing New State-run TLS Certificate Authority to Deal With Sanctions The Russian government has established its own TLS certificate authority (CA) to address issues with accessing websites that have arisen in the wake of sanctions imposed by the west following the country's unprovoked military invasion of Ukraine. According to a message posted on the Gosuslugi public services portal, the Ministry of Digital Development is expected to provide a domestic
 Naked Security	S3 Ep73: Ransomware with a difference, dirty Linux pipes, and much more [Podcast] Latest episode - listen now!	 Cyware News - Latest Cyber News SEC to vote on new cybersecurity disclosure rules as Ukraine crisis gives them 'special relevance' The proposed amendments will be put out for a public comment period, which will be either 30 days from when it is published in the Federal Register, or 60 days after it is issued, whichever is longer.
 Cyware News - Latest Cyber News	US Treasury: Russia may bypass sanctions using ransomware payments The Treasury Department's Financial Crimes Enforcement Network (FinCEN) warned U.S. financial institutions this week to keep an eye out for attempts to evade sanctions and US-imposed restrictions following Russia's invasion of Ukraine.	 Security Affairs Vodafone investigates claims of a data breach made by Lapsus\$ gang Vodafone is investigating a recently suffered cyberattack, after a ransomware gang Lapsus\$ claimed to have stolen its source code. Vodafone announced to have launched an investigation after the Lapsus\$ cybercrime group claimed to have stolen its source code. The Lapsus\$ gang claims to have stolen approximately 200 GB of source code files, allegedly contained in [...] The post Vodafone investigates claims of a data breach made by Lapsus\$ gang appeared first on Security Affairs.

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	 Dave Rubin This man slept with a Chinese spy and is now giving cybersecurity tips. Please fact check me, @twitter[...]
 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.	 Spiros Margaris The best #Indian #conferences for #womenintech in 2022 #fintech #cybersecurity @Analyticsindiam

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

NIST CVE: Low

NIST CVE: Unrated

CVE-2022-22141	<p>'Long-term Data Archive Package' service implemented in the following Yokogawa Electric products creates some named pipe with improper ACL configuration. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-11</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11	CVE-2022-22148	<p>'Root Service' service implemented in the following Yokogawa Electric products creates some named pipe with improper ACL configuration. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-11</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11
UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11								
UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11								
CVE-2022-25508	<p>An access control issue in the component /ManageRoute/postRoute of FreeTAKServer v1.9.8 allows unauthenticated attackers to cause a Denial of Service (DoS) via an unusually large amount of created routes, or create unsafe or false routes for legitimate users.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-11</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11	CVE-2022-25511	<p>An issue in the ?filename= argument of the route /DataPackageTable in FreeTAKServer-UI v1.9.8 allows attackers to place arbitrary files anywhere on the system.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-11</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11
UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11								
UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11								
CVE-2022-26662	<p>An XML Entity Expansion (XEE) issue was discovered in Tryton Application Platform (Server) 5.x through 5.0.45, 6.x through 6.0.15, and 6.1.x and 6.2.x through 6.2.5, and Tryton Application Platform (Command Line Client (proteus)) 5.x through 5.0.11, 6.x through 6.0.4, and 6.1.x and 6.2.x through 6.2.1. An unauthenticated user can send a crafted XML-RPC message to consume all the resources of the server.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-10</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-10	Updated: 2022-03-11	CVE-2022-26661	<p>An XXE issue was discovered in Tryton Application Platform (Server) 5.x through 5.0.45, 6.x through 6.0.15, and 6.1.x and 6.2.x through 6.2.5, and Tryton Application Platform (Command Line Client (proteus)) 5.x through 5.0.11, 6.x through 6.0.4, and 6.1.x and 6.2.x through 6.2.1. An authenticated user can make the server parse a crafted XML SEPA file to access arbitrary files on the system.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-10</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-10	Updated: 2022-03-11
UNRATED	Vector: unknown	Created: 2022-03-10	Updated: 2022-03-11								
UNRATED	Vector: unknown	Created: 2022-03-10	Updated: 2022-03-11								
CVE-2022-22151	<p>CAMS for HIS Log Server contained in the following Yokogawa Electric products fails to properly neutralize log outputs: CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, and Exaopc versions from R3.72.00 to R3.79.00.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-11</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11	CVE-2022-22145	<p>CAMS for HIS Log Server contained in the following Yokogawa Electric products is vulnerable to uncontrolled resource consumption. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-03-11</td><td>Updated: 2022-03-11</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11
UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11								
UNRATED	Vector: unknown	Created: 2022-03-11	Updated: 2022-03-11								
CVE-2022-22729	<p>CAMS for HIS Server contained in the following Yokogawa Electric products improperly authenticate the receiving packets. The authentication may be bypassed via some crafted packets: CENTUM CS 3000 versions from R3.08.10</p>	CVE-2022-0822	<p>Cross-site Scripting (XSS) - Reflected in</p>								

to R3.09.00, **CENTUM VP** versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, and **Exaopc** versions from R3.72.00 to R3.79.00.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

GitHub repository orchardcms/orchardcore prior to 1.3.0.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-0820

Cross-site Scripting (XSS) - Stored in **GitHub** repository orchardcms/orchardcore prior to 1.3.0.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-26878

drivers/bluetooth/virtio_bt.c in the **Linux** kernel before 5.16.3 has a memory leak (socket buffers have memory allocated but not freed).

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-25510

FreeTAKServer 1.9.8 contains a hardcoded **Flask** secret key which allows attackers to create crafted cookies to bypass authentication or escalate privileges.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-25506

FreeTAKServer-UI v1.9.8 was discovered to contain a SQL injection vulnerability via the API endpoint /AuthenticateUser.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-25507

FreeTAKServer-UI v1.9.8 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Callsign parameter.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-25512

FreeTAKServer-UI v1.9.8 was discovered to leak sensitive API and **Websocket** keys.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-0821

Improper Authorization in **GitHub** repository orchardcms/orchardcore prior to 1.3.0.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-0913

Integer Overflow or Wraparound in **GitHub** repository microweber/microweber prior to 1.3.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2020-36518

jackson-databind before 2.13.0 allows a **Java** StackOverflow exception and denial of service via a large depth of nested objects.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-26874

lib/Horde/Mime/Viewer/Ooo.php in Horde Mime_Viewer before 2.2.4 allows XSS via an **OpenOffice** document, leading to account takeover in Horde **Groupware Webmail** Edition. This occurs after XSLT rendering.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-21808

Path traversal vulnerability exists in CAMS for HIS Server contained in the following **Yokogawa** Electric products: **CENTUM CS 3000** versions from R3.08.10 to R3.09.00, **CENTUM VP** versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, **Exaopc** versions from R3.72.00 to R3.79.00.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2018-25031

Swagger UI before 4.1.3 could allow a remote attacker to conduct spoofing attacks. By persuading a victim to open a crafted URL, an attacker could exploit this vulnerability to display remote OpenAPI **definitions**.

UNRATED	Vector: unkown	Created: 2022-03-11	Updated: 2022-03-11
---------	-------------------	------------------------	------------------------

CVE-2022-23401

The following **Yokogawa** Electric products contain insecure DLL loading issues. **CENTUM CS 3000** versions from R3.08.10 to R3.09.00, **CENTUM VP** versions from

CVE-2022-21194

The following **Yokogawa** Electric products do not change the passwords of the internal **Windows** accounts from the initial configuration: **CENTUM VP** versions from

R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, **Exaopc** versions from R3.72.00 to R3.79.00.

UNRATEDVector: unknownCreated: 2022-03-11Updated: 2022-03-11

R5.01.00 to R5.04.20 and versions from R6.01.00 to R6.08.0, **Exaopc** versions from R3.72.00 to R3.79.00.

UNRATEDVector: unknownCreated: 2022-03-11Updated: 2022-03-11

CVE-2022-23402

The following **Yokogawa** Electric products hard-code the password for CAMS server applications: **CENTUM VP** versions from R5.01.00 to R5.04.20 and versions from R6.01.00 to R6.08.00, **Exaopc** versions from R3.72.00 to R3.79.00

UNRATEDVector: unknownCreated: 2022-03-11Updated: 2022-03-11

CVE-2021-46708

The swagger-ui-dist package before 4.1.3 for **Node.js** could allow a remote attacker to hijack the clicking **action** of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim.

UNRATEDVector: unknownCreated: 2022-03-11Updated: 2022-03-11

CVE-2022-21177

There is a path traversal vulnerability in CAMS for HIS **Log Server** contained in the following **Yokogawa** Electric products: **CENTUM CS 3000** versions from R3.08.10 to R3.09.00, **CENTUM VP** versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, andfrom R6.01.00 to R6.08.00, **Exaopc** versions from R3.72.00 to R3.79.00.

UNRATEDVector: unknownCreated: 2022-03-11Updated: 2022-03-11

CVE-2022-0912

Unrestricted Upload of File with Dangerous Type in **GitHub** repository microweber/microweber prior to 1.2.11.

UNRATEDVector: unknownCreated: 2022-03-11Updated: 2022-03-11





Source: [Hybrid Analysis](#)







Top malicious files

100% Threat score	EzYAOCTRT (.) exe	100% Threat score	CH00072991 _ 44068 _ SRL _ 11-03-2022 _ pdf (.) jar
100% Threat score	installDatashareStandalone (.) exe	100% Threat score	vapev4_installer (.) exe
100% Threat score	SQLi Dumper (.) exe	100% Threat score	New Order (.) exe
100% Threat score	fVVa9DXB	100% Threat score	360a712adc0fa8304a864b70a2026ec42d65fec062b065459769781a9114e259 (.) exe
82% Threat score	index2-ajax-response (.) php	80% Threat score	Condemned_Criminal_Origins_Turkce_Yama (.) exe
72% Threat score	IEExtensionInstaller (.) msi	71% Threat score	VirusShare_480ef02bb062a57724e1b3e14532a140

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 Brazil
	#9 Japan		#10 Uruguay





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 Thailand
	#5 Indonesia		#6 Algeria

			
	#7 Viet Nam		#8 Brazil
	#9 Iran (Islamic Republic of)		#10 Pakistan

Source: [SpamHaus](#)

Top phishing countries

	#1 United States		#2 Germany
	#3 Russia		#4 Singapore
	#5 Netherlands		#6 Iran
	#7 Indonesia		#8 Japan
	#9 Belgium		#10 Canada