Your Security Rabbits report for March 29, 2022

Hot topics

Nothing today

Source: Ransom Watch

Ransomware attacks

vicesociety	APSM Systems	vicesociety	ASPIRO
lockbit2	axessa,ch	alphv	Rudsak Inc | rudsak,com
vicesociety	Ciments Guyanais	conti	GRS Group
leaktheanalyst	18 Build your own drone	leaktheanalyst	19 You Must Never Forget LeakTheAnalyst
conti	Allied Eagle Supply	conti	AB Karl Hedin
lockbit2	bro	lockbit2	its,ws
conti	Neschen Coating GmbH	conti	ONCALL Language Services
vicesociety	OSSEG Obra Social del Seguro	lockbit2	progettoedilesr,,,
clop	SA1SOLUTIONS,COM FILES	clop	SLIMSTOCK,COM
stormous	Smith Transport company	clop	ZISSERFAMILYLAW,COM
leaktheanalyst	16 Nuclear leak	leaktheanalyst	10 Bearking News
vicesociety	Universidade Federal de Sao Paulo	leaktheanalyst	11 you're awake!
leaktheanalyst	12 Escape from the dark	leaktheanalyst	13 We are kids !
leaktheanalyst	14 Kids vs, Governments !	leaktheanalyst	15 All we know
leaktheanalyst	15,1 Supplementary	vicesociety	OSSEG Obra Social de Seguros
leaktheanalyst	1 Breaking News	leaktheanalyst	17 \"Shoulders! How shocking!\" Queen
leaktheanalyst	2 Breaking News	leaktheanalyst	3 Breaking News
leaktheanalyst	4 Breaking News	leaktheanalyst	5 Customer Leak and F5 destroying
leaktheanalyst	6 Under Attack	leaktheanalyst	7 Absurd Analysis
leaktheanalyst	8 Breaking News	leaktheanalyst	9 Cuz F5 has caused

News

IT Security Guru

86% of organisations believe they have suffered a nation-state cyberattack

A new study by Trellix and the Center for Strategic and International Studies (CSIS) has revealed that 86% of organisations believe they have fallen victim to a nation-state cyberattack. The research surveyed 800 IT decision-makers in Australia, France, Germany, India, Japan, the UK and US. It has also been revealed that 92% of respondents have faced, or suspect they […] The post 86% of organisations believe they have suffered a nation-state cyberattack appeared first on IT Security Guru.

Cyware News - Latest Cyber News

86% of Organizations Have Faced a Nation-State Cyber-Attack

Nearly nine in 10 (86%) organizations believe they have been targeted by a nation-state threat actor, according to a new study by Trellix and the Center for Strategic and International Studies (CSIS).

A Large-Scale Supply Chain Attack Distributed Over 800 Malicious NPM Packages

Anonymous is working on a huge data dump that will blow Russia away

The Hacker News

A threat actor dubbed "RED-LILI" has been linked to an ongoing large-scale supply chain attack campaign targeting the NPM package repository by publishing nearly 800 malicious modules. "Customarily, attackers use an anonymous disposable NPM account from which they launch their attacks," Israeli security company Checkmarx said. "As it seems this time, the attacker has fully-automated the process

Cyware News - Latest Cyber News

Attackers Use Compromised Philippine Navy Certificate to Spread Remote Access Tool

Avast Threat Intelligence Team has found a remote access tool (RAT) actively being used in the wild in the Philippines that uses what appears to be a compromised digital certificate belonging to the Philippine Navy.

Cyware News - Latest Cyber News

Chrome and Edge hit with V8 type confusion vulnerability with in-the-wild exploit

Google is urging users on Windows, macOS, and Linux to update Chrome builds to version 99.0.4844.84, following the discovery of a vulnerability that has an exploit in the wild.

Cyware News - Latest Cyber News

Cloud-native adoption shifts security responsibility across teams

As organizations increase cloud-native adoption, a new Styra report outlines why developers and IT decision-makers need a unified approach to address security and compliance issues.

IT Security Guru

Critically Exposed Web Apps Discovered Across Europe's Top Chemical Manufacturers

New research has revealed the top Chemical Manufacturers in the EU all have concerning levels of vulnerabilities and weak spots in their attack surface. According to the 2022 Web Application Security for Chemical Manufacturers report by Outpost24, 60% of European Chemical Manufacturers had vulnerabilities that are critically exposed and open to attacks. This new industry threat [...] The post Critically Exposed Web Apps Discovered Across Europe's Top Chemical Manufacturers appeared first on IT Security Guru.

The Hacker News

Experts Detail Virtual Machine Used by Wslink Malware Loader for Obfuscation

Cybersecurity researchers have shed more light on a malicious loader that runs as a server and executes received modules in memory, laying bare the structure of an "advanced multi-layered virtual machine" used by the malware to fly under the radar. Wslink, as the malicious loader is called, was first documented by Slovak cybersecurity company ESET in October 2021, with very few telemetry hits

Cyware News - Latest Cyber News

Hackers Hijack Email Reply Chains on Unpatched Exchange Servers to Spread IcedID Malware

A new email phishing campaign has been spotted leveraging the tactic of conversation hijacking to deliver the IcedID info-stealing malware onto infected machines by making use of unpatched and publicly-exposed Microsoft Exchange servers.

Security Affairs

Hive ransomware ports its encryptor to Rust programming language

The Hive ransomware gang ported its encryptor to the Rust programming language and implemented new features. The Hive ransomware operation has developed a Rust version of their encryptor and added new features to prevent curious from snooping on the victim's ransom negotiations. According to BleepingComputer, which focused on Linux VMware ESXi encryptor, the Hive ransomware [...] The post Hive ransomware ports its encryptor to Rust programming language appeared first on Security Affairs.

CyberScoop

Lack of speedy notification was 'a mistake,' Okta says

Okta says it should have acted sooner to explain what it knew, and when, about an incident at customer service contractor Sitel. The post Lack of speedy notification was 'a mistake,' Okta says appeared first on CyberScoop.

Cyware

Malware-as-a-Service Gains Prominence in Threat Landscape

While organizations have improved their backup strategy, ransomware groups are responding by exfiltrating sensitive data and threatening to expose it. Cybercriminals are still shifting to living-off-

Security Affairs

The Anonymous collective hacked the Russian construction company Rostproekt and announced that a leak that will Blow Russia Away. Anonymous continues its offensive against Russia, the collective announced the hack of the Russian construction company Rostproekt and announced a leak that will blow Russia away. Link to the stolen data from the company have been [...] The post Anonymous is working on a huge data dump that will blow Russia away appeared first on Security Affairs.

CyberScoop

Biden budget requests big increase for cybersecurity

DHS would get the biggest slice of the federal cybersecurity budget request at $2.6 billion. The post Biden budget requests big increase for cybersecurity appeared first on CyberScoop.

Security Affairs

CISA adds Chrome, Redis bugs to the Known Exploited Vulnerabilities Catalog

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added Chrome and Redis flaws to its Known Exploited Vulnerabilities Catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added Google Chome zero-day (CVE-2022-1096) and a critical Redis vulnerability (CVE-2022-0543), along with other 30 vulnerabilities, to its Known Exploited Vulnerabilities Catalog. According to Binding Operational Directive (BOD) 22-01: Reducing [...] The post CISA adds Chrome, Redis bugs to the Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

Threatpost

Critical Sophos Security Bug Allows RCE on Firewalls

The security vendor's appliance suffers from an authentication-bypass issue.

IT Security Guru

EU and US confirm transatlantic data flow

The new Trans-Atlantic Data Privacy Framework, announced over the weekend by the EU and the US, signals incoming clarification as to what data flows are allowed. The announcement comes after a European court struck down the EU-US Privacy Shield one and a half years ago. The Privacy Shield agreement, which set the terms for transatlantic transfers [...] The post EU and US confirm transatlantic data flow appeared first on IT Security Guru.

Naked Security

Google Chrome patches mysterious new zero-day bug - update now

CVE-2022-1096 - another mystery in-the-wild 0-day in Chrome... check your version now!

The Hacker News

Hackers Hijack Email Reply Chains on Unpatched Exchange Servers to Spread Malware

A new email phishing campaign has been spotted leveraging the tactic of conversation hijacking to deliver the IcedID info-stealing malware onto infected machines by making use of unpatched and publicly-exposed Microsoft Exchange servers. "The emails use a social engineering technique of conversation hijacking (also known as thread hijacking)," Israeli company Intezer said in a report shared with

ZDNet | security RSS

Hundreds more packages found in malicious npm 'factory'

Over 600 malicious packages were published in only five days.

IT Security Guru

Major League Baseball players' personal data stolen

A third-party vendor of American Major League Baseball has been hit with a cyber-attack, resulting in the personal information of players and their family members being stolen. Horizon Actuarial Services LLC, a consulting firm based in Maryland, suffered a ransomware attack in November of last year. The company recently released a data incident notice, revealing [...] The post Major League Baseball players' personal data stolen appeared first on IT Security Guru.

The Hacker News

New Malware Loader 'Verblecon' Infects Hacked PCs with Cryptocurrency Miners

An unidentified threat actor has been observed employing a "complex and powerful" malware loader with the ultimate objective of deploying cryptocurrency miners on compromised systems and potentially facilitating the theft of Discord tokens. "The evidence

News - Latest Cyber News

the-land attack techniques.

The Hacker News

New Report on Okta Hack Reveals the Entire Episode LAPSUS$ Attack
An independent security researcher has shared what's a detailed timeline of events that transpired as the notorious LAPSUS$ extortion gang broke into a third-party provider linked to the cyber incident at Okta in late January 2022. In a set of screenshots posted on Twitter, Bill Demirkapi published a two-page "intrusion timeline" allegedly prepared by Mandiant, the cybersecurity firm hired by

Cyware News - Latest Cyber News

Oklahoma City Indian Clinic impacted by Suncrypt's ransomware attack
The explanation for the "technological issues" appears to be a ransomware attack by Suncrypt, who have added the clinic to their dedicated leak site. Suncrypt claims that they have acquired 350GB+ of files.

Threatpost

Okta Says It Goofed in Handling the Lapsus$ Attack
"We made a mistake," Okta said, owning up to its responsibility for security incidents that hit its service providers and potentially its own customers.

Cyware News - Latest Cyber News

Phishing Kits Evolve and Evade Detection
Off-the-shelves, modern phishing kits are being sold on underground forums that contain several, sophisticated detection avoidance and traffic filtering processes to not be marked as threats. Fake websites impersonating renowned brands are created using phishing kits featuring realistic login pages, brand logos, and in special cases, dynamic web pages.

Cyware News - Latest Cyber News

SunCrypt ransomware is still alive and kicking in 2022
SunCrypt, a ransomware-as-a-service (RaaS) operation that reached prominence in mid-2020, is reportedly still active, even if barely, as its operators continue to work on giving its strain new capabilities.

CyberScoop

Ukrainian telecom, government blame cyberattack for most severe disruption since Russian invasion
The disruption targeted a large service provider in what might be the latest in a string of ongoing intentional internet disruptions. The post Ukrainian telecom, government blame cyberattack for most severe disruption since Russian invasion appeared first on CyberScoop.

WeLiveSecurity

Under the hood of Wslink's multilayered virtual machine
ESET researchers describe the structure of the virtual machine used in samples of Wslink and suggest a possible approach to see through its obfuscation techniques The post Under the hood of Wslink's multilayered virtual machine appeared first on WeLiveSecurity

IT Security Guru

US proposes healthcare cybersecurity bill
A new bill with bipartisan support has been proposed by US lawmakers, with the intention of enhancing the cybersecurity of America's healthcare and public health (HPH) sector. The Healthcare Cybersecurity Act (S.3904) was proposed by US senators Jacky Rosen and Bill Cassidy on Thursday. The proposal is likely a reaction to the White House warning […] The post US proposes healthcare cybersecurity bill appeared first on IT Security Guru.

found on victim networks appears to indicate that the goal of the attacker was to install cryptocurrency mining software on victim machines,"

The Hacker News

Of Cybercriminals and IP Addresses
You don't like having the FBI knocking on your door at 6 am in the morning. Surprisingly, nor does your usual cybercriminal. That is why they hide (at least the good ones), for example, behind layers of proxies, VPNs, or TOR nodes. Their IP address will never be exposed directly to the target's machine. Cybercriminals will always use third-party IP addresses to deliver their attacks. There are

Cyware News - Latest Cyber News

Okta acknowledges 'mistake' in handling of Lapsus$ attack
In an FAQ published last Friday, Okta offered a full timeline of the incident, starting from January 20 when the company learned "a new factor was added to a Sitel customer support engineer's Okta account."

Cyware News - Latest Cyber News

One in 10 UK Staff Circumvent Corporate Security
Part of the problem appears to be user friction in existing security measures. Less than half (44%) of those polled said they find it easy to securely access their IT equipment within minutes.

Cyware News - Latest Cyber News

Ransomware Attacks Soar by 100% in 2021
The number of ransomware attacks reported to the UK's data protection regulator more than doubled between 2020 and 2021 as the pandemic raged, according to a new analysis.

Blog â€“ Flashpoint

The Promise of Open Source Code and the Paradox of 'ProtestWare'
The Open Source Software (OSS) community has been split in two after an OSS author repurposed his own library to protest the Ukrainian-Russian war. On March 7, RIAEvangelist released several versions of his "node-ipc" software package--which has been downloaded millions of times--with some versions reportedly overwriting code on machines presumably located in Russia and Belarus. […] The post The Promise of Open Source Code and the Paradox of 'ProtestWare' appeared first on Flashpoint.

Security Affairs

Ukrtelecom, a major mobile service and internet provider in Ukraine, foiled a "massive" cyberattack that hit its infrastructure
Ukrtelecom, a major mobile service and internet provider in Ukraine, foiled a "massive" cyberattack that hit its infrastructure. On March 29, 2022, a massive cyber attack caused a major internet disruption across Ukraine on national provider Ukrtelecom. According to global internet monitor service NetBlock, real-time network data showed connectivity collapsed to 13% of pre-war levels. […] The post Ukrtelecom, a major mobile service and internet provider in Ukraine, foiled a "massive" cyberattack that hit its infrastructure appeared first on Security Affairs.

Cyware News - Latest Cyber News

Update: Hundreds more packages found in malicious npm 'factory'
On Monday, Checkmarx researchers said they have also been tracking these activities and have recorded over 600 malicious packages published over five days, bringing the total to over 700.

Security Affairs

While Twitter suspends Anonymous accounts, the group hacked VGTRK Russian Television and Radio
While Twitter suspends some Anonymous accounts, the collective hacked All-Russia State Television and Radio Broadcasting Company (VGTRK). On Friday, Anonymous announced that the affiliate group Black Rabbit World has leaked 28 GB of data stolen from the Central Bank of Russia. The group plans to distribute the stolen documents to various points on the internet […] The post While Twitter suspends Anonymous accounts, the group hacked VGTRK Russian Television and Radio 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

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

Dave Rubin

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

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

Gary Gensler

a discussion on cybersecurity disclosures.

Spiros Margaris

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

Source: Imperva DDOS Map

Top DDOS country targets

Source: Hybrid Analysis

Top malicious URL

Nothing today

Source: NIST

NIST CVE: Critical

CVE-2021-43735

CmsWing 1.3.7 is affected by a SQLi vulnerability via parameter: behavior rule.

CRITICAL Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-25222

Money Transfer Management System Version 1.0 allows an unauthenticated user to inject SQL queries in 'admin/maintenance/manage_branch.php' and 'admin/maintenance/manage_fee.php' via the 'id' parameter.

CRITICAL Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2021-43736

CmsWing CMS 1.3.7 is affected by a Remote Code Execution (RCE) vulnerability via parameter: log rule

CRITICAL Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-0888

The **Ninja Forms** - File Uploads Extension **WordPress** plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/includes/ajax/controllers/uploads.php file which can be bypassed making it possible for unauthenticated attackers to upload malicious files that can be used to obtain remote code execution, in versions up to and including 3.3.0

CRITICAL Vector: network Created: 2022-03-23 Updated: 2022-03-29

Source: NIST

NIST CVE: High

CVE-2021-43738

An issue was discovered in xiaohuanxiong CMS 5.0.17. There is a CSRF vulnerability that can that can add the administrator account.

HIGH Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2021-46064

IrfanView 4.59 is vulnerable to buffer overflow via the function at address 0x413c70 (in 32bit version of the binary). The vulnerability triggers when the user opens malicious .tiff image.

HIGH Vector: local Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-24775

guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds.

HIGH Vector: network Created: 2022-03-21 Updated: 2022-03-29

CVE-2021-44139

Sentinel 1.8.2 is vulnerable to Server-side request forgery (SSRF).

HIGH Vector: network Created: 2022-03-23 Updated: 2022-03-29

Source: NIST

NIST CVE: Medium

CVE-2022-0862

A lack of password change protection vulnerability in a depreciated API of **McAfee** Enterprise **ePolicy Orchestrator** (ePO) prior to 5.10 Update 13 allows a remote attacker to change the password of a compromised session without knowing the existing user's password. This functionality was removed from the User Interface in ePO 10 and the API has now been disabled. Other protection is in place to reduce the likelihood of this being successful through sending a link to a logged in user.

CVE-2021-4180

An information exposure flaw in openstack-tripleo-heat-templates allows an external user to **discover** the internal IP or hostname. An attacker could exploit this by checking the www_authenticate_uri parameter (which is visible to all end users) in configuration files. This would give sensitive information which may aid in additional system exploitation. This flaw affects openstack-tripleo-heat-templates versions prior to 11.6.1.

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2021-43737

An issus was discovered in xiaohuanxiong CMS 5.0.17. There is a CSRF vulnerability that can modify administrator account's password.

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-25221

Money Transfer Management System Version 1.0 allows an attacker to inject JavaScript code in the URL and then trick a user into visit the link in order to execute JavaScript code.

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-0834

The Amelia **WordPress** plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the lastName parameter found in the ~/src/Application/Controller/User/Customer/AddCustomerController.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a user accesses the booking calendar with the **date** the attacker has injected the malicious payload into. This affects versions up to and including 1.0.46.

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-0750

The Photoswipe Masonry **Gallery WordPress** plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the thumbnail_width, thumbnail_height, max_image_width, and max_image_height parameters found in the ~/photoswipe-masonry.php file which allows authenticated attackers to inject arbitrary web scripts into galleries created by the plugin and on the PhotoSwipe Options page. This affects versions up to and including 1.2.14.

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-27090

Cscms Music Portal System v4.2 was discovered to contain a **redirection** vulnerability via the backurl parameter.

MEDIUM Vector: network Created: 2022-03-21 Updated: 2022-03-29

CVE-2022-23242

TeamViewer Linux versions before 15.28 do not properly execute a deletion command for the connection password in case of a process crash. Knowledge of the crash event and the TeamViewer ID as well as either possession of the pre-crash connection password or local authenticated access to the machine would have allowed to establish a remote connection by reusing the not properly deleted connection password.

MEDIUM Vector: local Created: 2022-03-23 Updated: 2022-03-29

CVE-2022-0889

The **Ninja Forms** - File Uploads Extension **WordPress** plugin is vulnerable to reflected cross-site scripting due to missing sanitization of the files filename parameter found in the ~/includes/ajax/controllers/uploads.php file which can be used by unauthenticated attackers to add malicious web scripts to vulnerable WordPress sites, in versions up to and including 3.3.12.

MEDIUM Vector: network Created: 2022-03-23 Updated: 2022-03-29

Source: NIST

NIST CVE: Low

CVE-2022-0861

A XML Extended entity vulnerability in **McAfee** Enterprise **ePolicy Orchestrator** (ePO) prior to 5.10 Update 13 allows a remote administrator attacker to upload a malicious XML file through the extension import functionality. The impact is limited to some access to confidential information and some ability to alter data.

LOW Vector: network Created: 2022-03-23 Updated: 2022-03-29

Source: NIST

NIST CVE: Unrated

CVE-2022-27948

** DISPUTED ** Certain **Tesla** vehicles through 2022-03-26 allow attackers to open the charging port via a 315 MHz RF **signal** containing a fixed sequence of approximately one hundred symbols. NOTE: the vendor's perspective is that the behavior is as intended.

UNRATED Vector: unkown Created: 2022-03-27 Updated: 2022-03-29

CVE-2021-45866

A Stored Cross Site Scripting (XSS) vulnerability exists in **Sourcecodester** Student Attendance Management System 1.0 via the couse filed in index.php.

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

CVE-2022-1084

A vulnerability **classified** as critical was found in **SourceCodester** One Church Management System 1.0. Affected by this vulnerability is an unknown functionality of the file

CVE-2021-45865

A File Upload vulnerability exists in **Sourcecodester** Student Attendance Manageent System 1.0 via the file upload functionality.

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

CVE-2022-1083

A vulnerability **classified** as critical has been found in Microfinance Management System. The manipulation of arguments like customer_type_number/account_number/account_status_number/account_type_number with the input ' and (select * from(select(sleep(10)))Avx) and 'abc' = 'abc leads to sql injection in multiple files. It is possible to launch the attack remotely.

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

CVE-2022-1079

A vulnerability **classified** as problematic has been found in **SourceCodester** One

/one_church/userregister.php. The manipulation leads to authentication bypass. The attack can be launched remotely.

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

CVE-2022-1074 A vulnerability has been found in TEM FLEX-1085 1.6.0 and **classified** as problematic. Using the input HTML Injection in the WiFi settings of the dashboard leads to html injection.

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

CVE-2022-1076 A vulnerability was found in Automatic Question **Paper** Generator System 1.0. It has been **classified** as problematic. This affects the file /aqpg/users/login.php of the component My Account Page. The manipulation of the argument **First** Name/Middle Name/Last Name leads to cross site scripting. It is possible to initiate the attack remotely.

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

CVE-2022-1075 A vulnerability was found in College Website Management System 1.0 and **classified** as problematic. Affected by this issue is the file /cwms/classes/Master.php?f=save_contact of the component Contact Handler. The manipulation leads to persistent cross site scripting. The attack may be launched remotely and requires authentication.

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

CVE-2022-1078 A vulnerability was found in **SourceCodester** College Website Management System 1.0. It has been **classified** as critical. Affected is the file /cwms/admin/?page=articles/view_article/. The manipulation of the argument id with the input ' and (select * from(select(sleep(10)))Avx) and 'abc' = 'abc with an unknown input leads to sql injection. It is possible to launch the attack remotely and without authentication.

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

CVE-2022-1082 A vulnerability was found in **SourceCodester** Microfinance Management System 1.0. It has been rated as critical. This issue affects the file /mims/login.php of the Login Page. The manipulation of the argument username/password with the input '||1=1# leads to sql injection. The attack may be initiated remotely.

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

CVE-2022-1077 A vulnerability was found in TEM FLEX-1080 and FLEX-1085 1.6.0. It has been declared as problematic. This vulnerability log.cgi of the component Log Handler. A direct request leads to information disclosure of hardware information. The attack can be initiated remotely and does not require any form of authentication.

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

CVE-2022-0331 An information disclosure vulnerability in Webadmin allows an unauthenticated remote attacker to

Church Management System. Affected are multiple files and parameters which are prone to to cross site scripting. It is possible to launch the attack remotely.

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

CVE-2022-1073 A vulnerability was found in Automatic Question **Paper** Generator 1.0. It has been declared as critical. An attack leads to privilege escalation. The attack can be launched remotely.

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

CVE-2022-1085 A vulnerability was found in CLTPHP up to 6.0. It has been declared as problematic. Affected by this vulnerability is the POST Parameter Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.

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

CVE-2022-1086 A vulnerability was found in DolphinPHP up to 1.5.0 and **classified** as problematic. Affected by this issue is the User Management Page. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.

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

CVE-2022-1081 A vulnerability was found in **SourceCodester** Microfinance Management System 1.0. It has been declared as problematic. This vulnerability affects the file /mims/app/addcustomerHandler.php. The manipulation of the argument first_name, middle_name, and surname leads to cross site scripting. The attack can be initiated remotely.

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

CVE-2022-1080 A vulnerability was found in **SourceCodester** One Church Management System 1.0. It has been declared as critical. This vulnerability affects code of the file attendancy.php as the manipulation of the argument search2 leads to sql injection. The attack can be initiated remotely.

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

CVE-2022-1087 A vulnerability, which was **classified** as problematic, has been found in **htmly** 5.3 whis affects the component Edit Profile Module. The manipulation of the field Title with script tags leads to persistent cross site scripting. The attack may be initiated remotely and requires an authentication. A simple POC has been disclosed to the public and may be used.

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

CVE-2022-24956 An issue was discovered in **Shopware** B2B-Suite through 4.4.1. The sort-by read the device serial number in **Sophos Firewall** version v18.5 MR2 and older.

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

CVE-2021-44581

An SQL Injection vulnerabilty exists in Kreado Kreasfero 1.5 via the id parameter.

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

CVE-2021-46743

In Firebase PHP-JWT before 6.0.0, an algorithm-confusion issue (e.g., RS256 / HS256) exists via the kid (aka Key ID) header, when multiple types of keys are loaded in a key ring. This allows an attacker to **forge** tokens that validate under the incorrect key. NOTE: this provides a straightforward way to use the PHP-JWT library unsafely, but might not be considered a vulnerability in the library itself.

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

CVE-2022-1032

Insecure deserialization of not validated module file in **GitHub** repository crater-invoice/crater prior to 6.0.6.

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

CVE-2022-26269

Suzuki **Connect** v1.0.15 allows attackers to tamper with displayed messages via spoofed CAN messages.

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

parameter of the search functionality of b2border and b2borderlist allows SQL injection. Possible techniques are boolean-based blind, time-based blind, and potentially stacked queries. The vulnerability allows a remote authenticated attacker to dump the underlying database.

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

CVE-2022-24957

DHC **Vision** eQMS through 5.4.8.322 has Persistent XSS due to insufficient encoding of untrusted input/output. To exploit the vulnerability, the attacker has to create or edit a new information object and use the XSS payload as the name. Any user that opens the object's version or history tab will be attacked.

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

CVE-2022-23937

In Wind River **VxWorks** 6.9 and 7, a specific crafted packet may lead to an out-of-bounds read during an IKE initial **exchange** scenario.

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

CVE-2022-25420

NTT Resonant Incorporated goo **blog** App Web Application 1.0 is vulnerable to CLRF injection. This vulnerability allows attackers to execute arbitrary code via a crafted HTTP request.

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

CVE-2022-25521

UNNO v03.11.00 was discovered to contain access control issue.

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

Source: SpamHaus

Top spamming countries

Nothing today

Source: SpamHaus

Top spammers

Nothing today

Source: SpamHaus

Top countries with botnet

Nothing today

Source: SpamHaus

Top phishing countries

Nothing today

Source: Hybrid Analysis

Top malicious files

Nothing today

Source: Imperva DDOS Map

Top DDOS techniques

Source: Imperva DDOS Map

Top DDOS industry targets