Your Security Rabbits report for April 02, 2022

Source: Ransom Watch

Ransomware attacks

conti	FlipChip	lockbit2	ledesma.com.ar
lockbit2	liceu.barcelona	conti	MANUFAST
conti	GIBSON HomeWares	lockbit2	https://liceu.b...
conti	I-SEC International Security	conti	Midea Carrier

Hot topics

Nothing today

News

CyberScoop

'Spring4Shell' bug in framework for Java programming draws widespread warnings

Web applications created in the Spring platform could leave users open to remote code execution, CISA and others are warning. The post 'Spring4Shell' bug in framework for Java programming draws widespread warnings appeared first on CyberScoop.

Naked Security

"VMware Spring Cloud Function" Java bug gives instant remote code execution - update now!

Easy unauthenticated remote code execution - PoC code already out

The Hacker News

15-Year-Old Bug in PEAR PHP Repository Could've Enabled Supply Chain Attacks

A 15-year-old security vulnerability has been disclosed in the PEAR PHP repository that could permit an attacker to carry out a supply chain attack, including obtaining unauthorized access to publish rogue packages and execute arbitrary code. "An attacker exploiting the first one could take over any developer account and publish malicious releases, while the second bug would allow the attacker

Security Affairs

AcidRain, a wiper that crippled routers and modems in Europe

Researchers spotted a new destructive wiper, tracked as AcidRain, that is likely linked to the recent attack against Viasat. Security researchers at SentinelLabs have spotted a previously undetected destructive wiper, tracked as AcidRain, that hit routers and modems and that was suspected to be linked to the Viasat KA-SAT attack that took place on February [...] The post AcidRain, a wiper that crippled routers and modems in Europe appeared first on Security Affairs.

Security Affairs

Anonymous targets oligarchs' Russian businesses: Marathon Group hacked

Anonymous continues its operations against Russia, the group announced the hack of the Russian investment firm Marathon Group. Anonymous continues to target Russian firms owned by oligarchs, yesterday the collective announced the hack of the Thozis Corp, while today the group claimed the hack of Marathon Group. The Marathon Group is a Russian investment firm [...] The post Anonymous targets oligarchs' Russian businesses: Marathon Group hacked appeared first on Security Affairs.

Threatpost

Apple Rushes Out Patches for 0-Days in MacOS, iOS

The vulnerabilities could allow threat actors to disrupt or access kernel activity and may be under active exploit.

Cyware News - Latest Cyber News

Australian Government to Invest $9.9bn in Cyber

Dubbed REDSPICE, which stands for 'Resilience, Effects, Defense, Space, Intelligence, Cyber and Enablers,' it is the biggest single cybersecurity investment in Australian history.

The Hacker News

British Police Charge Two Teenagers Linked to LAPSUS$ Hacker Group

The City of London Police on Friday disclosed that it has charged two of the seven teenagers, a 16-year-old and a 17-year-old, who were arrested last week for their alleged connections to the LAPSUS$ data extortion gang. "Both teenagers have been charged with: three counts of unauthorized access to a computer with intent to impair the reliability of data; one count of fraud by false

ZDNet | security RSS

Chinese hackers Deep Panda return with Log4Shell exploits, new Fire Chili rootkit

Log4Shell is being exploited to deploy the kernel rootkit.

The Hacker News

Chinese Hackers Target VMware Horizon Servers with Log4Shell to Deploy Rootkit

A Chinese advanced persistent threat tracked as Deep Panda has been observed exploiting the Log4Shell vulnerability in VMware Horizon servers to deploy a backdoor and a novel rootkit on infected machines with the goal of stealing sensitive data. "The nature of targeting was opportunistic insofar that multiple infections in several countries and various sectors occurred on the same dates," said

The Hacker News

Critical Bugs in Rockwell PLC Could Allow Hackers to Implant Malicious Code

Two new security vulnerabilities have been disclosed in Rockwell Automation's programmable logic controllers (PLCs) and engineering workstation software that could be exploited by an attacker to inject malicious code on affected systems and stealthily modify automation processes. The flaws have the potential to disrupt industrial operations and cause physical damage to factories in a manner

Security Affairs

Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts

GitLab has addressed a critical vulnerability, tracked as CVE-2022-1162 (CVSS score of 9.1), that could allow remote attackers to take over user accounts. The CVE-2022-1162 vulnerability is related to the set of hardcoded static passwords during OmniAuth-based registration in GitLab CE/EE. "A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, [...] The post Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts appeared first on Security Affairs.

WeLiveSecurity

Cybersecurity survival tips for small businesses: 2022 edition

How can businesses that lack the resources and technological expertise of large organizations hold the line against cybercriminals? The post Cybersecurity survival tips for small businesses: 2022 edition appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

GitLab addresses critical account hijack bug

GitLab has patched a critical vulnerability that meant static passwords were inadvertently set during OmniAuth-based registration - putting accounts at risk of malicious takeover.

The Hacker

GitLab Releases Patch for Critical Vulnerability That Could Let Attackers Hijack Accounts

DevOps platform GitLab has released software updates to address a critical security vulnerability that, if potentially exploited, could permit an adversary to

Cyware

Hive Ransomware Ported to Rust, Encryptor Updated

Hive ransomware actors ported its Linux encryptor to Rust programming language to target VMware ESXi servers. Additionally, they have added new features to make it difficult for security researchers to snoop on victim's ransom

News

seize control of accounts. Tracked as CVE-2022-1162, the issue has a CVSS score of 9.1 and is said to have been discovered internally by the GitLab team. "A hardcoded password was set for accounts registered using an

IT Security Guru

Majority of data security incidents caused by insiders

New research from Imperva has revealed that 70% of EMEA organisations have no insider risk strategy, despite 59% of data security incidents being caused by employees. The shocking revelation comes as part of a wider study carried out by Forrester: Insider Threats Drive Data Protection Improvements. The study involved interviewing 150 security and IT professionals in EMEA. [...] The post Majority of data security incidents caused by insiders appeared first on IT Security Guru.

Cyware News - Latest Cyber News

NSA employee indicted for 'leaking top secret defense info'

The United States Department of Justice (DoJ) has accused an NSA employee of sharing top-secret national security information with an unnamed person who worked in the private sector.

Cyware News - Latest Cyber News

Phishing attacks exploit free calendar app to steal account credentials

In a recent report, email security provider INKY described a recent phishing campaign that took advantage of the Calendly calendar app to harvest sensitive account credentials from unsuspecting victims.

The Hacker News

Results Overview: 2022 MITRE ATT&CK Evaluation - Wizard Spider and Sandworm Edition

Threat actor groups like Wizard Spider and Sandworm have been wreaking havoc over the past few years - developing and deploying cybercrime tools like Conti, Trickbot, and Ryuk ransomware. Most recently, Sandworm (suspected to be a Russian cyber-military unit) unleashed cyberattacks against Ukranian infrastructure targets. To ensure cybersecurity providers are battle ready, MITRE Engenuity uses

Cyware News - Latest Cyber News

Russian-linked Android malware records audio, tracks your location

A previously unknown Android malware has been linked by the researchers to the Turla hacking group after discovering the app used infrastructure previously attributed to the threat actors.

Security Affairs

Trend Micro fixed high severity flaw in Apex Central product management console

Trend Micro has fixed a high severity arbitrary file upload flaw, tracked as CVE-2022-26871, in the Apex Central product management console. Cybersecurity firm Trend Micro has addressed a high severity security flaw, tracked as CVE-2022-26871, in the Apex Central product management console. The CVE-2022-26871 vulnerability is an arbitrary file upload issue, its exploitation could lead [...] The post Trend Micro fixed high severity flaw in Apex Central product management console appeared first on Security Affairs.

CyberScoop

Two alleged Lapsus$ teens appear in London court

Even after the arrests, the group has released more stolen data. The post Two alleged Lapsus$ teens appear in London court appeared first on CyberScoop.

Cyware News - Latest Cyber News

Verblecon: A New Advanced Malware Loader

A threat actor was spotted employing a sophisticated crypto-mining malware, dubbed Verblecon, on systems to steal access tokens for Discord chat app users. There are reports that connect a Verblecon domain to a ransomware attack as well. Organizations are recommended to use up-to-date and reliable anti-malware.

ZDNet | security RSS

Zyxel urges customers to patch critical firewall bypass vulnerability

The vendor has issued a severity score of 9.8.

Cyware News - Latest Cyber News

negotiations, which it appears to have copied from BlackCat. Organizations are advised focus on protecting sensitive data with robust encryption and access control.

The Hacker News

North Korean Hackers Distributing Trojanized DeFi Wallet Apps to Steal Victims' Crypto

The North Korean state-backed hacking crew, otherwise known as the Lazarus Group, has been attributed to yet another financially motivated campaign that leverages a trojanized decentralized finance (DeFi) wallet app to distribute a fully-featured backdoor onto compromised Windows systems. The app, which is equipped with functionalities to save and manage a cryptocurrency wallet, is also designed

Cyware News - Latest Cyber News

Ola Finance Says Attackers Stole $4.7M in 're-Entrancy' Exploit

Decentralized lending platform Ola Finance was exploited for over $4.67 million in a "re-entrancy" cyberattack, according to a post-mortem report released by the developers.

Cyware News - Latest Cyber News

Phishing Attacks Target NATO and European Military

Google TAG found multiple cybercriminal activities, such as phishing and malware attacks, targeting NATO and Eastern European countries. An APT group adopted a novel Browser-in-the-Browser (BitB) phishing technique. A group with alleged links to China targeted government and military organizations in Russia, Ukraine, Mongolia, and Kazakhstan.

The Hacker News

Russian Wiper Malware Likely Behind Recent Cyberattack on Viasat KA-SAT Modems

The cyberattack aimed at Viasat that temporarily knocked KA-SAT modems offline on February 24, 2022, the same day Russian military forces invaded Ukraine, is believed to have been the consequence of wiper malware, according to the latest research from SentinelOne. The findings come a day after the U.S. telecom company disclosed that it was the target of a multifaceted and deliberate" cyberattack

Cyware News - Latest Cyber News

Scammers are Exploiting Ukraine Donations

Scammers are exploiting the current events in Ukraine especially after the official Ukrainian Twitter account tweeted Bitcoin and Ethereum wallet addresses for donations.

Cyware News - Latest Cyber News

Trend Micro Patches Apex Central Zero-Day Exploited in Targeted Attacks

Trend Micro this week announced patches for a high-severity arbitrary file upload vulnerability in Apex Central that has already been exploited in what appear to be targeted attacks.

IT Security Guru

UK spy chief praises fake news counter cell

Jeremy Fleming, the head of GCHQ, has praised the new government counter-disinformation cell focused on Kremlin propaganda. Fleming spoke at the Australian National University in Canberra yesterday, arguing that President Putin had massively miscalculated his invasion Ukraine. He revealed that Russian soldiers are "refusing to carry out orders, sabotaging their own equipment and even accidentally [...] The post UK spy chief praises fake news counter cell appeared first on IT Security Guru.

Cyware News - Latest Cyber News

WordPress Popunder Malware Redirects to Scam Sites

The malware is always injected into the active theme's footer.php file, and contains obfuscated JavaScript after a long series of empty lines in an attempt to stay hidden.

Twitter

Rep. Mike Garcia

America must keep its eye on China. While chaos ensues around the globe, China remains the greatest threat to our nation's security. China failed to report the COVID-19 outbreak, they continue to threaten our cybersecurity, and they are watching Taiwan.

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

Nothing today

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2022-21830
A blind self XSS vulnerability exists in RocketChat LiveChat
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-23247
A command injection vulerability found in quick game engine allows arbitrary remote code in quick app. Allows remote attacke0rs to gain arbitrary code execution in quick game engine
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-27223
A denial-of-service issue existed in one of modules that was incorporated in **Kaspersky Anti-Virus** products for home and Kaspersky **Endpoint Security**. A local user could cause **Windows** crash by running a specially crafted binary module. The fix was delivered automatically. Credits: (Straghkov Denis, Kurmangaleev Shamil, Fedotov Andrey, Kuts Daniil, Mishechkin Maxim, Akolzin Vitaliy) @ ISPRAS
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2020-25691
A flaw was found in darkhttpd. Invalid error handling allows remote attackers to cause denial-of-service by accessing a file with a large modification **date**. The highest threat from this vulnerability is to system availability.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32957
A function in MDT **AutoSave** versions prior to v6.02.06 is used to retrieve system information for a specific process, and this information collection executes multiple commands and summarizes the information into an XML. This function and subsequent process gives full path to the executable and is therefore vulnerable to binary hijacking.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-27177
A **Python** format string issue leading to information disclosure and potentially remote code execution in ConsoleMe for all versions prior to 1.2.2
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22965
A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on **Tomcat** as a WAR deployment. If the application is deployed as a **Spring Boot** executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32945
An attacker could decipher the encryption and gain access to MDT **AutoSave** versions prior to v6.02.06.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32949
An attacker could utilize a function in MDT **AutoSave** versions prior to v6.02.06 that permits changing a designated path to another path and traversing the directory, allowing the replacement of an existing file with a malicious file.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-0489
An issue has been discovered in **GitLab** CE/EE affecting all versions starting with 8.15 . It was possible to trigger a DOS by using the math feature with a specific formula in issue comments.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-26624
An local privilege escalation vulnerability due to a "runasroot" command in eScan **Anti-Virus**. This vulnerability is due to invalid arguments and insufficient execution conditions related to "runasroot" command. This vulnerability can induce remote attackers to exploit root privileges by manipulating parameter values.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25159
Authentication Bypass by Capture-replay vulnerability in Mitsubishi Electric **MELSEC iQ-F** series FX5U(C) CPU all versions and Mitsubishi

CVE-2022-22570
A buffer overflow vulnerability found in the **UniFi** Door Access **Reader** Lite's (UA Lite) firmware (Version 3.8.28.24 and earlier) allows a malicious actor who has gained access to a network to control all connected UA devices. This vulnerability is fixed in Version 3.8.31.13 and later.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-26565
A cross-site scripting (XSS) vulnerability in **Totaljs** commit 95f54a5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page Name text field when creating a new page.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-0425
A DNS rebinding vulnerability in the Irker IRC Gateway integration in all versions of **GitLab** CE/EE since version 7.9 allows an attacker to trigger Server Side Request Forgery (SSRF) attacks.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-3461
A flaw was found in **keycloak** where keycloak may fail to logout user session if the logout request comes from external SAML **identity provider** and Principal Type is set to Attribute [Name].
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32961
A getfile function in MDT **AutoSave** versions prior to v6.02.06 enables a user to supply an optional parameter, resulting in the processing of a request in a special manner. This can result in the execution of an **unzip** command and place a malicious .exe file in one of the locations the function looks for and get execution capabilities.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-26623
A remote code execution vulnerability due to incomplete check for 'xheader_decode_path_record' function's parameter length value in the ark library. Remote attackers can induce exploit malicious code using this function.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32937
An attacker can gain knowledge of a session temporary working folder where the getfile and putfile commands are used in MDT **AutoSave** versions prior to v6.02.06. An attacker can leverage this knowledge to provide a malicious command to the working directory where the read and write activity can be initiated.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32933
An attacker could leverage an API to pass along a malicious file that could then manipulate the process creation command line in MDT **AutoSave** versions prior to v6.02.06 and run a command line argument. This could then be leveraged to run a malicious process.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32953
An attacker could utilize SQL commands to create a new user MDT **AutoSave** versions prior to v6.02.06 and update the user's permissions, granting the attacker the ability to login.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-26562
An issue in provider/libserver/ECKrbAuth.cpp of Kopano-Core v11.0.2.51 contains an issue which allows attackers to authenticate even if the user account or password is expired.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-3847
An unauthorized access to the execution of the setuid file with capabilities flaw in the **Linux** kernel OverlayFS subsystem was found in the way user copying a capable file from a nosuid mount into another mount. A local user could use this flaw to escalate their privileges on the system.
UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25158
Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric **MELSEC iQ-F** series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series **FX5UJ** CPU all versions allows a remote

Electric MELSEC iQ-F series **FX5UJ** CPU all versions allows a remote unauthenticated attacker to login to the product by replay attack.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25160

Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric **MELSEC iQ-F** series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series **FX5UJ** CPU all versions allows a remote unauthenticated attacker to disclose a file in a legitimate user's product by using previously eavesdropped cleartext information and to counterfeit a legitimate user's system.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32970

Data can be copied without validation in the built-in web server in **Moxa** NPort IAW5000A-I/O series firmware version 2.2 or earlier, which may allow a remote attacker to cause denial-of-service conditions.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-23155

Dell Wyse **Management Suite** versions 2.0 through 3.5.2 contain an unrestricted file upload vulnerability. A malicious user with admin privileges can exploit this vulnerability in order to execute arbitrary code on the system.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32976

Five buffer overflows in the built-in web server in **Moxa** NPort IAW5000A-I/O series firmware version 2.2 or earlier may allow a remote attacker to initiate a denial-of-service attack and execute arbitrary code.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22332

IBM Sterling Partner Engagement Manager 6.2.0 could allow an attacker to impersonate another user due to missing revocation mechanism for the JWT token. IBM X-Force ID: 219131.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22331

IBM SterlingPartner Engagement Manager 6.2.0 could allow a remote authenticated attacker to obtain sensitive information or modify user details caused by an insecure direct object vulnerability (IDOR). IBM X-Force ID: 219130.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-0373

Improper access control in **GitLab** CE/EE versions 12.4 to 14.5.4, 14.5 to 14.6.4, and 12.6 to 14.7.1 allows project non-members to retrieve the **service desk** email address

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-0741

Improper input validation in all versions of **GitLab** CE/EE using **sendmail** to send emails allowed an attacker to steal environment variables via specially crafted email addresses.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-22277

Improper Input Validation vulnerability in ABB 800xA, Control Software for AC 800M, Control Builder Safe, Compact Product Suite - Control and I/O, ABB **Base Software** for SoftControl allows an attacker to cause the denial of service.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22963

In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local **resources**.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-20238

It was found in **OpenShift** Container Platform 4 that **ignition** config, served by the Machine Config Server, can be accessed externally from clusters without authentication. The MCS endpoint (port 22623) provides ignition configuration used for bootstrapping Nodes and can include some sensitive data, e.g. **registry** pull secrets. There are two scenarios where this data can be accessed. The **first** is on Baremetal, OpenStack, Ovirt, **Vsphere** and **KubeVirt** deployments which do not have a separate internal API endpoint and allow access from outside the cluster to port 22623 from the standard OpenShift API Virtual IP address. The second is on cloud deployments when using unsupported network plugins, which do not create **iptables** rules that prevent to port 22623. In this scenario, the ignition config is exposed to all **pods** within the cluster and cannot be accessed externally.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-27534

Kaspersky Anti-Virus products for home and Kaspersky **Endpoint Security** with **antivirus** databases released before 12 March 2022 had a bug in a data parsing module that potentially allowed an attacker to execute arbitrary code. The fix was delivered automatically. Credits: Georgy Zaytsev (Positive Technologies).

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

attacker to disclose or tamper with a file in which password hash is saved in cleartext.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-24181

Cross-site scripting (XSS) via Host Header injection in PKP Open Journals System 2.4.8 >= 3.3 allows remote attackers to inject arbitary code via the X-Forwarded-Host Header.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-24426

Dell Command | Update, Dell Update, and Alienware Update versions prior to 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-1098

Delta Electronics DIAEnergie (all versions prior to 1.8.02.004) are vulnerable to a DLL hijacking condition. When combined with the Incorrect Default Permissions vulnerability of 4.2.2 above, this makes it possible for an attacker to escalate privileges

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22404

IBM App Connect Enterprise Certified Container Dashboard UI (IBM **App Connect Enterprise Certified Container** 1.5, 2.0, 2.1, 3.0, and 3.1) may be vulnerable to denial of service due to excessive rate limiting.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22328

IBM SterlingPartner Engagement Manager 6.2.0 could allow a malicious user to elevate their privileges and perform unintended operations to another users data. IBM X-Force ID: 218871.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22327

IBM UrbanCode **Deploy** (UCD) 7.0.5, 7.1.0, 7.1.1, and 7.1.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 218859.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-0390

Improper access control in **Gitlab** CE/EE versions 12.7 to 14.5.4, 14.6 to 14.6.4, and 14.7 to 14.7.1 allowed for project non-members to retrieve issue details when it was linked to an item from the vulnerability dashboard.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32974

Improper input validation in the built-in web server in **Moxa** NPort IAW5000A-I/O series firmware version 2.2 or earlier may allow a remote attacker to execute commands.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-39908

In all versions of **GitLab** CE/EE, certain **Unicode** characters can be abused to commit malicious code into projects without being noticed in **merge** request or source code viewer UI.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-20295

It was discovered that the update for the virt:rhel module in the RHSA-2020:4676 (https://access.redhat.com/errata/RHSA-2020:4676) erratum released as part of Red Hat **Enterprise Linux** 8.3 failed to include the fix for the qemu-kvm component issue CVE-2020-10756, which was previously corrected in virt:rhel/qemu-kvm via erratum RHSA-2020:4059 (https://access.redhat.com/errata/RHSA-2020:4059). CVE-2021-20295 was assigned to that Red Hat specific security regression. For more details about the original security issue CVE-2020-10756, refer to bug 1835986 or the CVE page: https://access.redhat.com/security/cve/CVE-2020-10756.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2019-14839

It was observed that while login into Business-central console, HTTP request discloses sensitive information like username and password when intercepted using some tool like **burp** suite etc.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-1068

Modbus Tools **Modbus Slave** (versions 7.4.2 and prior) is vulnerable to a stack-based buffer overflow in the registration field. This may cause the program to crash when a long character string is used.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-22950

n **Spring Framework** versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-26417

Omron CX-Position (versions 2.5.3 and prior) is vulnerable to a use after free memory condition while processing a specific project file, which may allow an attacker to execute arbitrary code.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25959

Omron CX-Position (versions 2.5.3 and prior) is vulnerable to memory corruption while processing a specific project file, which may allow an attacker to execute arbitrary code.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-28504

On **Arista** Strata family products which have "TCAM profile" feature enabled when Port IPv4 access-list has a rule which matches on "vxlan" as protocol then that rule and subsequent rules (rules declared after it in ACL) do not match on IP protocol field as expected.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-44135

pagekit all versions, as of 15-10-2021, is vulnerable to SQL Injection via Comment listing.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-27501

Philips Vue PACS versions 12.2.x.x and prior does not follow certain coding rules for development, which can lead to resultant weaknesses or increase the severity of the associated vulnerabilities.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-33024

Philips Vue PACS versions 12.2.x.x and prior transmits or stores authentication credentials, but it uses an insecure method susceptible to unauthorized interception and/or retrieval.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-33020

Philips Vue PACS versions 12.2.x.x and prior uses a cryptographic key or password past its expiration date, which diminishes its **safety** significantly by increasing the timing window for cracking attacks against that key.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-1159

Rockwell **Automation Studio** 5000 Logix **Designer** (all versions) are vulnerable when an attacker who achieves administrator access on a **workstation** running **Studio 5000 Logix Designer** could inject controller code undetectable to a user.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-27306

The function url.parse() in **Node.js** v17.7.0 allows attackers to spoof a hostname.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-21223

The package cocoapods-downloader before 1.6.2 are vulnerable to Command Injection via hg argument injection. When calling the download function (when using hg), the url (and/or revision, tag, branch) is passed to the hg clone command in a way that additional flags can be set. The additional flags can be used to perform a command injection.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-24066

The package simple-git before 3.5.0 are vulnerable to Command Injection due to an incomplete fix of [CVE-2022-24433] (https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2421199) which only patches against the git fetch attack vector. A similar use of the --upload-pack feature of git is also supported for git clone, which the prior fix didn't cover.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-33018

The use of a broken or risky cryptographic algorithm in **Philips** Vue PACS versions 12.2.x.x and prior is an unnecessary risk that may result in the exposure of sensitive information.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-23287

The vulnerability exists due to insufficient validation of input of certain **resources** within the IPM software. This issue affects: **Intelligent Power Manager** (IPM 1) versions prior to 1.70.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-1201

NULL Pointer Dereference in mrb_vm_exec with super in **GitHub** repository mruby/mruby prior to 3.2. This vulnerability is capable of making the mruby interpreter crash, thus affecting the availability of the system.

UNRATED Vector: unkown Created: 2022-04-02 Updated: 2022-04-02

CVE-2022-26022

Omron CX-Position (versions 2.5.3 and prior) is vulnerable to an out-of-bounds write while processing a specific project file, which may allow an attacker to execute arbitrary code.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-26419

Omron CX-Position (versions 2.5.3 and prior) is vulnerable to multiple stack-based buffer overflow conditions while parsing a specific project file, which may allow an attacker to locally execute arbitrary code.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-1207

Out-of-bounds read in **GitHub** repository radareorg/radare2 prior to 5.6.8. This vulnerability allows attackers to read sensitive information from outside the allocated buffer boundary.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-27493

Philips Vue PACS versions 12.2.x.x and prior does not ensure or incorrectly ensures structured messages or data are well formed and that certain security properties are met before being read from an upstream component or sent to a downstream component.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-27497

Philips Vue PACS versions 12.2.x.x and prior does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-33022

Philips Vue PACS versions 12.2.x.x and prior transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32960

Rockwell Automation **FactoryTalk Services Platform** v6.11 and earlier, if FactoryTalk Security is enabled and deployed contains a vulnerability that may allow a remote, authenticated attacker to bypass FactoryTalk Security policies based on the computer name. If successfully exploited, this may allow an attacker to have the same privileges as if they were logged on to the client machine.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2020-14479

Sensitive information can be obtained through the handling of serialized data. The issue results from the lack of proper authentication required to query the server

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-24440

The package cocoapods-downloader before 1.6.0, from 1.6.2 and before 1.6.3 are vulnerable to Command Injection via git argument injection. When calling the Pod::Downloader.preprocess_options function and using git, both the git and branch parameters are passed to the git ls-remote subcommand in a way that additional flags can be set. The additional flags can be used to perform a command injection.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-21235

The package **github**.com/masterminds/vcs before 1.13.3 are vulnerable to Command Injection via argument injection. When hg is executed, argument strings are passed to hg in a way that additional flags can be set. The additional flags can be used to perform a command injection.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-0922

The software does not perform any authentication for critical system functionality.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-23288

The vulnerability exists due to insufficient validation of input from certain **resources** by the IPP software. The attacker would need access to the local Subnet and an administrator interaction to compromise the system. This issue affects: Intelligent Power Protector versions prior to 1.69.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-33657

There is a heap overflow problem in video/SDL_pixels.c in SDL (Simple DirectMedia Layer) 2.x to 2.0.18 versions. By crafting a malicious .BMP file, an attacker can cause the application using this library to crash, denial of service or Code execution.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32968

Two buffer overflows in the built-in web server in **Moxa** NPort IAW5000A-I/O Series firmware version 2.2 or earlier may allow a remote attacker to cause a denial-of-service condition.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2021-32503

Unauthenticated users can access sensitive web URLs through GET request, which should be restricted to maintenance users only. A malicious attacker could use this sensitive information's to launch further attacks on the system.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25157

Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric **MELSEC iQ-F** series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series **FX5UJ** CPU all versions allows a remote unauthenticated attacker to disclose or tamper with the information in the product by using an eavesdropped password hash.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25155

Use of Password Hash Instead of Password for Authentication vulnerability in Mitsubishi Electric **MELSEC iQ-F** series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series **FX5UJ** CPU all versions allows a remote unauthenticated attacker to login to the product by replaying an eavesdropped password hash.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-25156

Use of Weak Hash vulnerability in Mitsubishi Electric **MELSEC iQ-F** series FX5U(C) CPU all versions and Mitsubishi Electric MELSEC iQ-F series **FX5UJ** CPU all versions allows a remote unauthenticated attacker to login to the product by using a password reversed from a previously eavesdropped password hash.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-1018

When opening a malicious solution file provided by an attacker, the application suffers from an XML external entity vulnerability due to an unsafe call within a dynamic link library file. An attacker could exploit this to pass data from local files to a remote web server, leading to a loss of confidentiality.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-23157

Wyse **Device Agent** version 14.6.1.4 and below contain a sensitive data exposure vulnerability. A authenticated malicious user could potentially exploit this vulnerability in order to view sensitive information from the WMS Server.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-23158

Wyse **Device Agent** version 14.6.1.4 and below contain a sensitive data exposure vulnerability. A local authenticated user with standard privilege could potentially exploit this vulnerability and provide incorrect port information and get connected to valid WMS server

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

CVE-2022-23156

Wyse **Device Agent** version 14.6.1.4 and below contain an Improper Authentication vulnerability. A malicious user could potentially exploit this vulnerability by providing invalid input in order to obtain a connection to WMS server.

UNRATED Vector: unkown Created: 2022-04-01 Updated: 2022-04-02

Source: Hybrid Analysis

Top malicious files

100% Threat score	MyJio For Everything Jio v7.0.06 Premium Mod Apk {CracksHash}.apk	100% Threat score	cain_abel_E04w-C1.exe
100% Threat score	tmpipvz8az_	100% Threat score	1b9a300d4e882a59e4bb15f7aa7069df6cc48057d1f89a71fff6df4e70d483f1.exe
100% Threat score	Spammer.exe	100% Threat score	tmpy13481ke
96% Threat score	Lucky Patcher v10.1.0 Premium Mod Apk {CracksHash}.apk	91% Threat score	Escape.exe
82% Threat score	app1094829.apk	78% Threat score	d347e095369aba294f674331054df8469b12d5e3260deb168827142d862f88d6
75% Threat score	AutoKeyPresserSetup.exe		

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://www.lrbss.com/
85% Threat score	http://globaltextiles.net/cgi-bin/7naWzYGRrrN/
82% Threat score	http://transmail.ftrans01.com/USQDEPCZN?id=67766%3DcE9VBgNRAQMHTF5QVAAKVAMEAwdcAQBTBlBUVgAEDghSB10EAFYAVAUBAFdRVVBXUVFJBA1VDAABVlQMAHZRVFJaCRhWCVtJAAYMW1ZUAgJUBwNRCFsOCQ
74% Threat score	https://www.joma.biz/profile/voir-hd-morbius-film-complet-720p-gratuits/profile
74% Threat score	https://freestuffbot.xyz/redirect/elden-ring-free-promotion-53129936/#ELDEN-RING
74% Threat score	https://lacapitaldelsol.com/anuncio/ver-fresh-2022-online-y-pelis-espanol-disney-4k-ultra-hd/
74% Threat score	https://www.lrbss.com/
74% Threat score	https://cncbrasil.art.br/community/profile/123ver-los-tipos-malos-2022-pelicula-completa/

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 Venezuela (Bolivarian Republic of)

Source: SpamHaus

Top phishing countries

#1 United States	#2 Germany
#3 Australia	#4 Russia
#5 Netherlands	#6 Japan
#7 Singapore	#8 India

#9 Hong Kong

#10 Bulgaria

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (30%)

Germany (18%)

Singapore (12%)

Source: Imperva DDOS Map

Top DDOS country targets

Russia (45%)

United States (17%)

Ukraine (15%)

Source: Imperva DDOS Map

Top DDOS techniques

59% **DDoS**

29% **Automated Threat**

12% **OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

52% **Financial Services**

20% **Business**

8% **Computing & IT**