Your Security Rabbits report for March 12, 2022

Source: Ransom Watch

Ransomware attacks

arvinclub	Target: bedfordshire . police . uk(2022-03-12)
lockbit2	Target: snteseccion30sa . . . (2022-03-12)
alphv	Target: inibsa . com | inibsadental . com | inibsa . net(2022-03-12)
lockbit2	Target: cachibi . co(2022-03-12)
lockbit2	Target: sysmac . com . sg(2022-03-11)
lockbit2	Target: weber-betonpump . . (2022-03-11)
lockbit2	Target: bioskin . sg(2022-03-10)
lockbit2	Target: bridgestoneamer . . . (2022-03-09)
conti	Target: Aluminerie Alouette(2022-03-09)
conti	Target: Myron Corp . (2022-03-08)
lockbit2	Target: ymcad(2022-03-12)
lockbit2	Target: orientalaromati . . . (2022-03-12)
lockbit2	Target: etg . digital(2022-03-12)
everest	Target: SPERONI SpA(2022-03-11)
lockbit2	Target: tingtong . com . cn(2022-03-11)
lockbit2	Target: fer(2022-03-10)
conti	Target: Great HealthWorks(2022-03-09)
conti	Target: TST Logistics(2022-03-09)
lockbit2	Target: hamm(2022-03-08)
everest	Target: XEFI(2022-03-08)

Hot topics

Nothing today

News

Cyware News - Latest Cyber News

287,652 South Denver Cardiology Associates patients notified of breach
In a notice on their website, the South Denver Cardiology Associates noted that there was no impact to the contents of patient medical records and no unauthorized access to the patient portal.

Security Affairs

Anonymous hacked Roskomnadzor agency revealing Russian disinformation
The Anonymous collective continues to launch attacks against Russian entities, this is a summary of recent offensives. Anonymous announced to have hacked the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media, also known as Roskomnadzor. The agency is responsible for monitoring, controlling and censoring Russian mass media and according to Anonymous, […] The post Anonymous hacked Roskomnadzor agency revealing Russian disinformation appeared first on Security Affairs.

Cyware

Attackers Created Terabytes of DDoS Attack Traffic Using a Single Packet
Researchers from a number of organizations confirmed

Naked Security

Alleged Kaseya ransomware attacker arrives in Texas for trial
The US Independence Day weekend of 2021 wasn't much of a holiday for cybersecurity staff. That was when the Kaseya attack unfolded...

Cyware News - Latest Cyber News

Anonymous Hacks Russian Media Censoring Agency Roskomnadzor
The international hacktivists collective Anonymous has struck again and this time the group is claiming to have hacked Roskomnadzor, a major Russian federal agency. The group also claims to have stolen over 360,000 files.

Didi said to halt Hong Kong listing plan on cyber security probe

News - Latest Cyber News

that attackers have been exploiting Mitel enterprise collaboration products to amplify DDoS attacks by 4 billion times from a single packet. The researchers recommend updating the systems with the latest patches. Additionally, Mitel users can detect and block inappropriate incoming traffic on UDP port 10074 with standard network defense tools.

Blog â€“ Flashpoint

Funding and the Russia-Ukraine War: KYC for Crypto Transactions Proving Difficult

Click here for Flashpoint's coverage of the role of intelligence in Russia's war on Ukraine. Flashpoint analysts have uncovered 262 cryptocurrency addresses used in advertisements for donations to either Ukrainian or Russian causes related to the war since February 21, 2022. As the Russian invasion of Ukraine draws more need for financial contributions to fund military and [...] The post Funding and the Russia-Ukraine War: KYC for Crypto Transactions Proving Difficult appeared first on Flashpoint.

IT Security Guru

High rates of known, exploitable vulnerabilities still found in the wild, report reveals

This week, smart vulnerability management provider Edgescan has published the findings of its 2022 Vulnerability Statistics Report, which for the 7th year running offers a comprehensive view of the state of vulnerability management globally. The report reveals that organizations are still taking nearly two months to remediate critical risk vulnerabilities, with the average mean time [...] The post High rates of known, exploitable vulnerabilities still found in the wild, report reveals appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Lapsus$ Ransomware Group Announces Hiring of Insiders from Tech Giants, ISPs, and Telcos

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.

Cyware News - Latest Cyber News

LockBit ransomware gang claims attack on Bridgestone Americas

No details about the incident emerged until the LockBit ransomware gang claimed the attack by adding Bridgestone Americas to the list of their victims. The threat actor announced that they will leak all data stolen and launched a countdown timer.

The Hacker News

Multiple Security Flaws Discovered in Popular Software Package Managers

Multiple security vulnerabilities have been disclosed in popular package managers that, if potentially exploited, could be abused to run arbitrary code and access sensitive information, including source code and access tokens, from compromised machines. It's, however, worth noting that the flaws require the targeted developers to handle a malicious package in conjunction with one of the affected

Threatpost

Raccoon Stealer Crawls Into Telegram

The credential-stealing trash panda is using the chat app to store and update C2 addresses as crooks find creative new ways to distribute the malware.

Threatpost

Russia Issues Its Own TLS Certs

The country's citizens are being blocked from the internet because foreign certificate authorities can't accept payments due to Ukraine-related sanctions, so it created its own CA.

Russia to create its own security certificate authority, alarming experts

Cyware News - Latest Cyber News

Didi Global has suspended preparations for its planned Hong Kong listing after failing to appease Chinese regulators' demands that it overhaul its systems for handling sensitive user data, according to unnamed sources.

Cyware News - Latest Cyber News

Hacked US Companies to Face New Reporting Requirements

The rules are part of a broader effort by the Biden administration and Congress to shore up the nation's cyber defenses after a series of high-profile digital espionage campaigns and disruptive ransomware attacks.

Cyware News - Latest Cyber News

High-Severity Vulnerabilities Patched in Omron PLC Programming Software

Several high-severity vulnerabilities that can be exploited for remote code execution were patched recently in the CX-Programmer software of Japanese electronics giant Omron.

Cyware News - Latest Cyber News

Leaked Conti files reveal life inside ransomware gang

Conti extorted an estimated $180m last year, making it the most lucrative ransomware operation of 2021, according to the latest Crypto Crime Report from security shop Chainanysis.

CyberScoop

Major cyber incident reporting requirement, CISA budget hike on precipice of becoming law

The incident reporting legislation, long in the works, also comes with nearly $2.6 billion for the agency for fiscal 2022. The post Major cyber incident reporting requirement, CISA budget hike on precipice of becoming law appeared first on CyberScoop.

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.

Krebs on Security

Report: Recent 10x Increase in Cyberattacks on Ukraine

As their cities suffered more intense bombardment by Russian military forces this week, Ukrainian Internet users came under renewed cyberattacks, with one Internet company providing service there saying they blocked ten times the normal number of phishing and malware attacks targeting Ukrainians.

Threatpost

Russia May Use Ransomware Payouts to Avoid Sanctions' Financial Harm

FinCEN warns financial institutions to be ware of unusual cryptocurrency payments or illegal transactions Russia may use to ease financial hurt from Ukraine-linked sanctions.

SafeBase bags $18M Series A to speed up vendor security auditing process

CyberScoop

Russia responds to economic sanctions hobbling renewals of its Internet security certificates by saying it will create its own. The post Russia to create its own security certificate authority, alarming experts appeared first on CyberScoop.

Cyware News - Latest Cyber News

Toei Animation Suffers Cyberattack Delaying Release of New ONE PIECE Anime Episodes

Anime giant Toei suffered unauthorized access to their systems on Mach 6th, 2022, causing delays in airing new episodes of popular anime series, including ONE PIECE and Delicious Party Precure.

Cyware News - Latest Cyber News

Ukrainian IT Army Hijacked by Info-stealing Malware

Security researchers at Cisco Talos are urging pro-Ukrainian actors to be wary of downloading DDoS tools to attack Russia, as they may be booby-trapped with info-stealing malware.

Cyware News - Latest Cyber News

Wightlink Reports Potential Data Breach After Suffering Highly Sophisticated Cyberattack

In a statement obtained by The Daily Swig, Wightlink said: "Unfortunately, despite Wightlink taking appropriate security measures, some of its back-office IT systems were affected by a cyber-attack last month.

Cyware News - Latest Cyber News

The company, which allows clients to share their security posture with customers, announced an $18 million Series A investment led by New Enterprise Associates, with participation from Y Combinator and Comcast Ventures.

Security Affairs

Ubisoft suffered a cyber security incident that caused a temporary disruption

Video game company Ubisoft has suffered a 'cyber security incident' that had a severe impact on games, systems, and services. The rumors of a cyber attack against Ubisoft circulated online in the last few days, while data extortion group LAPSUS$ claimed to have hacked the company. Over the last few days, multiple users reported problems accessing [...] The post Ubisoft suffered a cyber security incident that caused a temporary disruption appeared first on Security Affairs.

Blog â€“ Flashpoint

Understanding Russia's "Sovereign Internet": What Happens If Russia Isolates Itself from the Global Internet?

Click here for Flashpoint's coverage of the role of intelligence in Russia's war on Ukraine. Russia moves to control the information narrative The Russian government ordered state-owned portals to connect to its state-controlled domain name system servers by March 11--and, to switch to Russian hosting providers and localize elements that may not in the future [...] The post Understanding Russia's "Sovereign Internet": What Happens If Russia Isolates Itself from the Global Internet? appeared first on Flashpoint.

Twitter

Rep. Val Demings

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

Gary Gensler

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

Dave Rubin

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

Spiros Margaris

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

Source: NIST

NIST CVE: Critical

CVE-2021-44629

A Buffer Overflow vulnerabilitiy exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/register feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.

CRITICAL	Vector: network	Created: 2022-03-10	Updated: 2022-03-12

CVE-2021-44622

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/check_reg_verify_code function which could let a remove malicious user execute arbitrary code via a crafted post request.

CRITICAL	Vector: network	Created: 2022-03-10	Updated: 2022-03-12

CVE-2021-44625

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in /cloud_config/cloud_device/info interface, which allows a malicious user to executee arbitrary code on the system via a crafted post request.

CRITICAL	Vector: network	Created: 2022-03-10	Updated: 2022-03-12

CVE-2021-44626

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/get_reg_verify_code feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.

CRITICAL	Vector: network	Created: 2022-03-10	Updated: 2022-03-12

CVE-2021-44627

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/get_reset_pwd_veirfy_code feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-44631

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/reset_cloud_pwd feature, which allows malicous users to execute arbitrary code on the system via a crafted post request.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-44623

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 via the /cloud_config/router_post/check_reset_pwd_verify_code interface.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2020-14115

A command injection vulnerability exists in the **Xiaomi** Router **AX3600**. The vulnerability is caused by a lack of inspection for incoming data detection. Attackers can exploit this vulnerability to execute code.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-46384

https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: RCE. The impact is: execute arbitrary code (remote). The attack vector is: ${"freemarker.template.utility.Execute"?new()("calc")}. PP MCMS has a pre-auth RCE vulnerability through which allows unauthenticated attacker with network access via http to compromise MCMS. Successful attacks of this vulnerability can result in takeover of MCMS.

CRITICAL Vector: network Created: 2022-03-04 Updated: 2022-03-12

CVE-2021-44630

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/modify_account_pwd feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-44632

A Buffer Overflow vulnerability exists in **TP-LINK** WR-886N 20190826 2.3.8 in the /cloud_config/router_post/upgrade_info feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-44628

A Buffer Overflow vulnerabiltiy exists in **TP-LINK** WR-886N 20190826 2.3.8 in thee /cloud_config/router_post/login feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.

CRITICAL Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25312

An XML external entity (XXE) injection vulnerability was discovered in the Any23 RDFa XSLTStylesheet extractor and is known to affect Any23 versions < 2.7. XML external entity injection (also known as XXE) is a **web security** vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the **application server** filesystem, and to **interact** with any back-end or external systems that the application itself can access. This issue is fixed in **Apache** Any23 2.7.

CRITICAL Vector: network Created: 2022-03-05 Updated: 2022-03-12

Source: NIST

NIST CVE: High

CVE-2021-27756

"TLS-RSA cipher suites are not disabled in **BigFix** Compliance up to v2.0.5. If TLS 2.0 and secure ciphers are not enabled then an attacker can passively record traffic and later decrypt it."

HIGH Vector: network Created: 2022-03-04 Updated: 2022-03-12

CVE-2021-22783

A CWE-200: Information Exposure vulnerability exists which could allow a session hijack when the door panel is communicating with the door. Affected Product: Ritto Wiser Door (All versions)

HIGH Vector: Created: Updated:

CVE-2020-14111

A command injection vulnerability exists in the **Xiaomi** Router **AX3600**. The vulnerability is caused by a lack of inspection for incoming data detection. Attackers can exploit this vulnerability to execute code.

HIGH Vector: local Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-38296

Apache Spark supports end-to-end encryption of RPC connections via "spark.authenticate" and "spark.network.crypto.enabled". In versions 3.1.2 and earlier, it uses a **bespoke** mutual authentication protocol that allows for full encryption key recovery. After an initial interactive attack, this would allow someone to decrypt plaintext traffic offline. Note that this does not affect security mechanisms controlled by "spark.authenticate.enableSaslEncryption", "spark.io.encryption.enabled", "spark.ssl", adjacent_network 2022-03-09 2022-03-12

CVE-2022-24734

MyBB is a free and open source forum software. In affected versions the Admin CP's Settings management module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type `php` with PHP code, executed on on _Change Settings_ pages. This results in a Remote Code Execution (RCE) vulnerability. The vulnerable module requires Admin CP access with the `Can manage settings?` permission. MyBB's Settings module, which allows administrators to add, edit, and delete non-default settings, stores setting data in an options code string ($options_code; mybb_settings.optionscode database column) that identifies the setting type and its options, separated by a new line character (\n). In MyBB 1.2.0, support for setting type php was added, for which the remaining part of the options code is PHP code executed on Change Settings pages (reserved for **plugins** and internal use). MyBB 1.8.30 resolves this issue. There are no known workarounds.

HIGH Vector: network Created: 2022-03-09 Updated: 2022-03-12

CVE-2020-36123

saitoha **libsixel** v1.8.6 was discovered to contain a double free via the component sixel_chunk_destroy at /root/libsixel/src/chunk.c.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25557

Tenda AX1806 v1.0.0.1 was discovered to contain a heap overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the urls parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25558

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetProvince. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ProvinceCode parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25549

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsEn parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25546

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsUser parameter.

Vector: Created: 2022- Updated: 2022-

"spark.ui.strictTransportSecurity". Update to Apache Spark 3.1.3 or later

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-0813

PhpMyAdmin 5.1.1 and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. This affects the lang parameter, the pma_parameter, and the **cookie** section.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-24753

Stripe CLI is a command-line tool for the Stripe **eCommerce** platform. A vulnerability in Stripe CLI exists on **Windows** when certain commands are run in a directory where an attacker has planted files. The commands are `stripe login`, `stripe config -e`, `stripe community`, and `stripe open`. **MacOS** and **Linux** are unaffected. An attacker who successfully exploits the vulnerability can run arbitrary code in the context of the current user. The update addresses the vulnerability by throwing an error in these situations before the code can run.Users are advised to upgrade to version 1.7.13. There are no known workarounds for this issue.

HIGH Vector: local Created: 2022-03-09 Updated: 2022-03-12

CVE-2022-25552

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ssid parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25551

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsDomain parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25553

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsPwd parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25555

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ntpServer parameter.

Vector: Created: 2022- Updated: 2022-

HIGH network 03-10 03-12

CVE-2022-25548

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the serverName parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25554

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceId parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25566

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-32008

This issue affects: **Secomea** GateManager Version 9.6.621421014 and all prior versions. Improper Limitation of a Pathname to restricted directory, allows logged in GateManager admin to delete system Files or Directories.

HIGH Vector: network Created: 2022-03-04 Updated: 2022-03-12

HIGH network 03-10 03-12

CVE-2022-25547

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25550

Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceName parameter.

HIGH Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-23915

The package **weblate** from 0 and before 4.11.1 are vulnerable to Remote Code Execution (RCE) via argument injection when using git or **mercurial** repositories. Authenticated users, can change the behavior of the application in an unintended way, leading to command execution.

HIGH Vector: network Created: 2022-03-04 Updated: 2022-03-12

Source: NIST

NIST CVE: Medium

CVE-2021-33851

A cross-site scripting (XSS) attack can cause arbitrary code (JavaScript) to run in a user's browser and can use an application as the vehicle for the attack. The XSS payload given in the "Custom logo link" executes whenever the user opens the Settings Page of the "Customize Login Image" Plugin.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-24322

A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a disruption of communication between the Modicon controller and the engineering software when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure **Control Expert** (V15.0 SP1 and prior)

MEDIUM Vector: network Created: 2022-03-09 Updated: 2022-03-12

CVE-2021-32434

abcm2ps v8.14.11 was discovered to contain an out-of-bounds read in the function calculate_beam at **draw**.c.

MEDIUM Vector: local Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-33852

A cross-site scripting (XSS) attack can cause arbitrary code (JavaScript) to run in a user's browser and can use an application as the vehicle for the attack. The XSS payload given in the "Duplicate Title" text box executes whenever the user opens the Settings Page of the Post **Duplicator** Plugin or the application root page after duplicating any of the existing posts.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-24323

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a disruption of communication between the Modicon controller and the engineering software, when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure Process Expert (V2021 and prior), EcoStruxure **Control Expert** (V15.0 SP1 and prior)

MEDIUM Vector: network Created: 2022-03-09 Updated: 2022-03-12

CVE-2021-46353

An information disclosure in **web interface** in **D-Link** DIR-X1860 before 1.03 RevA1 allows a remote unauthenticated attacker to send a specially crafted HTTP request and gain knowledge of different absolute paths that are being used by the web application.

MEDIUM Vector: network Created: 2022-03-04 Updated: 2022-03-12

CVE-2022-26484

An issue was discovered in **Veritas InfoScale**

CVE-2022-26483

An issue was discovered in **Veritas InfoScale Operations Manager** (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. A reflected cross-site scripting (XSS) vulnerability in admin/cgi-bin/listdir.pl allows authenticated remote administrators to inject arbitrary web script or HTML into an HTTP GET parameter (which reflect the user input without sanitization).

MEDIUM Vector: network Created: 2022-03-04 Updated: 2022-03-12

CVE-2021-32436

An out-of-bounds read in the function write_title() in subs.c of **abcm2ps** v8.14.11 allows remote attackers to cause a Denial of Service (DoS) via unspecified vectors.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-25106

D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer overflow via the function genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload.

MEDIUM Vector: local Created: 2022-03-04 Updated: 2022-03-12

CVE-2021-28488

Ericsson Network Manager 20.2 has Insecure Permissions.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-34340

Ming 0.4.8 has an out-of-bounds buffer access issue in the function decompileINCR_DECR() in decompiler.c file that causes a direct segmentation fault and leads to denial of service.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-34338

Ming 0.4.8 has an out-of-bounds buffer overwrite issue in the function getName() in decompiler.c file that causes a direct segmentation fault and leads to denial of service.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-34342

Ming 0.4.8 has an out-of-bounds read vulnerability in the function newVar_N() in decompile.c which causes a huge information leak.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2022-0022

Usage of a weak cryptographic algorithm in Palo Alto Networks **PAN-OS** software where the password hashes of administrator and local user accounts are not created with a sufficient level of computational effort, which allows for password cracking attacks on accounts in normal (non-FIPS-CC) operational mode. An attacker must have access to the account password hashes to take advantage of this weakness and can acquire those hashes if they are able to gain access to the PAN-OS **software configuration**. Fixed versions of

Operations Manager (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. The web server fails to sanitize admin/cgi-bin/rulemgr.pl/getfile/ input data, allowing a remote authenticated administrator to read arbitrary files on the system via Directory Traversal. By manipulating the resource name in GET requests referring to files with absolute paths, it is possible to access arbitrary files stored on the filesystem, including application source code, configuration files, and critical system files.

MEDIUM Vector: network Created: 2022-03-04 Updated: 2022-03-12

CVE-2021-32005

Cross-site Scripting (XSS) vulnerability in log view of **Secomea SiteManager** allows a logged in user to store javascript for later execution. This issue affects: Secomea SiteManager Version 9.6.621421014 and all prior versions.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-43590

Dell EMC **Enterprise Storage** Analytics for vRealize Operations, versions 4.0.1 to 6.2.1, contain a Plain-text password storage vulnerability. A local high privileged malicious user may potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.

MEDIUM Vector: local Created: 2022-03-04 Updated: 2022-03-12

CVE-2020-14112

Information Leak Vulnerability exists in the **Xiaomi** Router AX6000. The vulnerability is caused by incorrect routing configuration. Attackers can exploit this vulnerability to download part of the files in Xiaomi Router AX6000.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-34339

Ming 0.4.8 has an out-of-bounds buffer access issue in the function getString() in decompiler.c file that causes a direct segmentation fault and leads to denial of service.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-34341

Ming 0.4.8 has an out-of-bounds read vulnerability in the function decompileIF() in the decompile.c file that causes a direct segmentation fault and leads to denial of service.

MEDIUM Vector: network Created: 2022-03-10 Updated: 2022-03-12

CVE-2021-32435

Stack-based buffer overflow in the function get_key in parse.c of **abcm2ps** v8.14.11 allows remote attackers to cause a Denial of Service (DoS) via unspecified vectors.

MEDIUM Vector: local Created: 2022-03-10 Updated: 2022-03-12

PAN-OS software use a secure cryptographic algorithm for account password hashes. This issue does not impact **Prisma** Access firewalls. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.21; All versions of PAN-OS 9.0; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11; PAN-OS 10.0 versions earlier than PAN-OS 10.0.7.

MEDIUM Vector: local Created: 2022-03-09 Updated: 2022-03-12

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-44667

A Cross Site Scripting (XSS) vulnerability exists in **Nacos** 2.0.3 in auth/users via the (1) pageSize and (2) pageNo parameters.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-26276

An issue in index.php of OneNav v0.9.14 allows attackers to perform directory traversal.

UNRATED Vector: unkown Created: 2022-03-12 Updated: 2022-03-12

CVE-2021-41848

An issue was discovered in Luna Simo PPR1.180610.011/202001031830. It mishandles software updates such that local third-party apps can provide a spoofed software update file that contains an arbitrary shell script and arbitrary ARM binary, where both will be executed as the root user with an **SELinux** domain named osi. To exploit this vulnerability, a local third-party app needs to have write access to external storage to write the spoofed update at the expected path. The vulnerable system binary (i.e., /system/bin/osi_bin) does not perform any authentication of the update file beyond ensuring that it is encrypted with an AES key (that is hard-coded in the vulnerable system binary). Processes executing with the osi SELinux domain can programmatically perform the following actions: install apps, grant **runtime** permissions to apps (including permissions with protection levels of dangerous and development), access extensive Personally Identifiable Information (PII) using the programmatically grant permissions, uninstall apps, set the default **launcher** app to a malicious launcher app that spoofs other apps, set a **network proxy** to intercept network traffic, **unload** kernel modules, set the default keyboard to a keyboard that has keylogging functionality, examine notification contents, send text messages, and more. The spoofed update can optionally contain an arbitrary ARM binary that will be locally stored in internal storage and executed at system startup to achieve persistent code execution as the root user with the osi SELinux domain. This ARM binary will continue to execute at startup even if the app that provided the spoofed update is uninstalled.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-26533

Alist v2.1.0 and below was discovered to contain a cross-site scripting (XSS) vulnerability via /i/:data/ipa.plist.

UNRATED Vector: unkown Created: 2022-03-12 Updated: 2022-03-12

CVE-2021-41850

An issue was discovered in Luna Simo PPR1.180610.011/202001031830. A pre-installed app with a package name of com.skyroam.silverhelper writes **three** IMEI values to system properties at system startup. The system property values can be obtained via getprop by all third-party applications co-located on the device, even those with no permissions granted, exposing the IMEI values to processes without enforcing any access control.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2021-41849

An issue was discovered in Luna Simo PPR1.180610.011/202001031830. It sends the following Personally Identifiable Information (PII) in plaintext using HTTP to servers located in China: user's list of installed apps and device International Mobile Equipment Identity (IMEI). This PII is transmitted to log.skyroam.com.cn using HTTP, **independent** of whether the user uses the Simo software.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2021-42577

An issue was discovered in **Softing** OPC UA C++ SDK before 5.70. A malformed OPC/UA message abort packet makes the client crash with a NULL pointer dereference.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-0880

Cross-site Scripting (XSS) - Stored in **GitHub** repository star7th/showdoc prior to 2.10.2.

UNRATED Vector: unkown Created: 2022-03-12 Updated: 2022-03-12

CVE-2022-24416

Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-24420

Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-0926

File upload filter bypass leading to stored XSS in **GitHub** repository microweber/microweber prior to 1.2.12.

UNRATED Vector: unkown Created: 2022-03-12 Updated: 2022-03-12

CVE-2022-24754

PJSIP is a free and open source multimedia communication library written in C language. In versions prior to and including 2.12 PJSIP there is a stack-buffer overflow vulnerability which only impacts PJSIP users who accept hashed digest credentials (credentials with data_type `PJSIP_CRED_DATA_DIGEST`). This issue has been patched in the master branch of the PJSIP repository and will be included with the next release. Users unable to upgrade need to check that the hashed digest data length must be equal to `PJSIP_MD5STRLEN` before passing to PJSIP.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2021-42262

An issue was discovered in **Softing** OPC UA C++ SDK before 5.70. An invalid XML element in the type dictionary makes the OPC/UA client crash due to an out-of-memory condition.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-24415

Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-24419

Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-24421

Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

CVE-2022-24760

Parse Server is an open source http web server backend. In versions prior to 4.10.7 there is a Remote Code Execution (RCE) vulnerability in Parse Server. This vulnerability affects Parse Server in the default configuration with **MongoDB**. The main weakness that leads to RCE is the Prototype Pollution vulnerable code in the file `DatabaseController.js`, so it is likely to affect Postgres and any other database backend as well. This vulnerability has been confirmed on **Linux** (Ubuntu) and **Windows**. Users are advised to upgrade as soon as possible. The only known workaround is to manually patch your installation with code referenced at the source GHSA-p6h4-93qp-jhcm.

UNRATED Vector: unkown Created: 2022-03-12 Updated: 2022-03-12

CVE-2022-25839

The package url-js before 2.1.0 are vulnerable to Improper Input Validation due to improper parsing, which makes it is possible for the hostname to be spoofed. http://\\\\\\\\localhost and http://localhost are the same URL. However, the hostname is not parsed as localhost, and the backslash is reflected as it is.

UNRATED Vector: unkown Created: 2022-03-11 Updated: 2022-03-12

Source: Hybrid Analysis

Top malicious files

100%
Threat score

PERFORMING VESSEL_MV (.) AGRICORE TBN (.) docx (.) exe

100%
Threat score

mlwr (.) bin

100%
Threat score

OTTSetup_0 (.) 87 (.) 6 (.) exe

100%
Threat score

XP-0897FD1B (.) EXE

100% Threat score	Internet (.) Download (.) Manager (.) v6 (.) 40 (.) 7 (.) exe
100% Threat score	megumi_final (.) dll
100% Threat score	CR_Downloader_for_sonic-the-hedgehog-(mega-play)_v3 (.) 06 (.) 414 (.) 64 (.) 35 (.) exe
100% Threat score	latest (.) exe
100% Threat score	Misc Ware v1 (.) 1 (.) exe
100% Threat score	7da4487d62a6800179765c4eebdbf764872a8325245bc5b77a9dcd318c22f7a4
100% Threat score	MemberPortal (.) pdf
95% Threat score	Porofessor (.) gg - Installer (.) exe
85% Threat score	setup-istripper_ruFVWIrshzVip5ZQZ32a4 (.) exe
81% Threat score	TGKDLL (.) dll
80% Threat score	Tester (.) exe
77% Threat score	n3xviruz (.) exe
76% Threat score	n3xviruz (.) exe
76% Threat score	getmacadress (.) exe
75% Threat score	Kiwi Application Monitor 1 (.) 5 (.) 3 (.) msi

Source: Hybrid Analysis

Top malicious URL

100% Threat score	https://ticketbud (.) com/events/1514f79e-a1dd-11ec-9e1b-42010a717019?preview=true&vox=true
100% Threat score	https://ticketbud (.) com/events/39f19492-a1dc-11ec-9882-42010a717019?preview=true&vox=true
96% Threat score	http://melekler (.) atspace (.) cc/tests/JZm4UmD/
95% Threat score	http://gotovacoil (.) com/created/Protected%20Client (.) vbs
94% Threat score	http://124 (.) 114 (.) 128 (.) 122:4076/Mozi (.) m
79% Threat score	http://triple3designs (.) com/
79% Threat score	https://ticketbud (.) com/events/ff09425a-a1d9-11ec-8f3a-42010a717019?preview=true&vox=true
79% Threat score	https://trk (.) cp20 (.) com/click/d80o-2id9vg-wo07k5-ihzzodp1/
78% Threat score	http://nizwe (.) petttok (.) com/ashish (.) rajvanshi@adani (.) in
77% Threat score	https://trk (.) cp20 (.) com/click/d80o-2icqec-wmdwyg-ihzzodp3/
75% Threat score	http://f-r-i-d-g-e (.) tk/
75% Threat score	http://loko-architecten (.) nl/8606935E6826FD13AB6F770AA9FB41A6/HYTBhMFhi3bJ7/
74% Threat score	https://ticketbud (.) com/events/07903a36-a1db-11ec-b3a7-42010a717019?preview=true&vox=true
72% Threat score	http://password (.) dervisogluet (.) com/main/

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 Iran (Islamic Republic of)

#9 Brazil

#10 Pakistan

Source: SpamHaus

Top phishing countries

#1 United States

#2 Germany

#3 Russia

#4 Netherlands

#5 France

#6 Singapore

#7 Bulgaria

#8 Japan

#9 Canada

#10 India

Source: Have I been pwned?

Have I been pwnd

Nothing today

Source: Imperva DDOS Map

Top DDOS attackers

United States (15%)

Germany (13%)

United Kingdom (9%)

Source: Imperva DDOS Map

Top DDOS country targets

Ukraine (49%)

Russia (40%)

United States (4%)

Source: Imperva DDOS Map

Top DDOS techniques

87%	**DDoS**
7%	**Automated Threat**
6%	**OWASP**

Source: Imperva DDOS Map

Top DDOS industry targets

50%	**Business**
44%	**Financial Services**
2%	**Computing & IT**