Security Rabbits

# Your Security Rabbits report for February 17, 2022

## Hot topics

***Nothing today***

## News

CyberScoop

'Russian state-sponsored cyber actors' cited in hacks of U.S. defense contractors
For more than two years, "Russian state-sponsored cyber actors" have targeted the emails and other data of U.S. defense contractors that handle sensitive information about weapons development, computer systems, intelligence-gathering technology and more, the federal government warned Wednesday. The alert from the Cybersecurity and Infrastructure Security Agency said cleared defense contractors (CDCs) are the primary victims of the breaches. Those companies are authorized by the Department of Defense to access, receive and store classified information as part of their contracting work. The alert does not say whether classified information was accessed. The attackers, however, have been able t[...]

Cyware News - Latest Cyber News

Backup Plays Key Role in Ransomware Response, But Not a Complete Solution
Ransomware attacks have increased in volume, sophistication and ransom demanded consistently over the last few years. According to published records, the education and retail sector are most targeted.

Cyware News - Latest Cyber News

BlackByte Ransomware Attacks Target U.S. Critical Infrastructure, FBI Warns
US officials released a joint advisory against the BlackByte ransomware actors who are exploiting a known Exchange Server bug to target critical infrastructure. The advisory identifies BlackByte as a RaaS targeting Windows systems, both physical and virtual servers. The advisory by the FBI should be considered seriously and organizations must raise their security barriers high to face threats such as BlackByte.

ZDNet | security RSS

Businessman admits to working as spyware broker in US and Mexico
He pleaded guilty to brokering spyware and surveillance tools.

Threatpost

Critical VMware Bugs Open ESXi, Fusion & Workstation to Attackers
A group of five security vulnerabilities could lead to a range of bad outcomes for virtual-machine enthusiasts, including command execution and DoS.

Threatpost

Emotet Now Spreading Through Malicious Excel Files
An ongoing malicious email campaign that includes macro-laden files and multiple layers of obfuscation has been active since late December.

WeLiveSecurity

Folding the impossible into the reality of normal life
Progress is a driving force of humanity, but what does that word "progress" really mean and what part do we have to play? The post Folding the impossible into the reality of normal life appeared first on WeLiveSecurity

Cyware News - Latest Cyber News

Google Drive Now Accounts for 50% of Malicious Document Downloads
According to Atlas VPN, nearly 50% of malicious Office documents were downloaded from Google Drive in 2021. Until 2020, Microsoft OneDrive was the major source of malicious office documents at 34% share. Cybercriminals spread these by creating free accounts on cloud apps hosting services, upload malicious files and share them publicly or with selected individuals. Organizations must secure their cloud apps with user authentication and threat monitoring tools.

Threatpost

High-Severity RCE Bug Found in Popular Apache Cassandra Database
On the plus side, only instances with non-standard not recommended configurations are vulnerable. On the downside, those configurations aren't easy to track down, and it's easy as pie to exploit.

CISA Alerts

AA22-047A: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
Actions to Help Protect Against Russian State-Sponsored Malicious Cyber Activity: * Enforce multifactor authentication. * Enforce strong, unique passwords. * Enable M365 Unified Audit Logs. * Implement endpoint detection and response tools. From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resour[...]

IT Security Guru

Baltimore tricked out of $375k
The Office of the Inspector General (OIG) has released a report revealing that Baltimore city was tricked out of hundreds of thousands of dollars last year by a cyber-criminal posing as a vendor. After receiving information from Baltimore's Bureau of Accounting and Payroll Services (BAPS) in regards to a suspected fraudulent Electronic Funds Transfer (EFT), [...] The post Baltimore tricked out of $375k appeared first on IT Security Guru.

IC3.gov News

Business Email Compromise: Virtual Meeting Platforms

Cyware News - Latest Cyber News

CISA Identifies Next Set of Actively Exploited Vulnerabilities
The CISA has added more flaws in its catalog of known exploited vulnerabilities. They were found in products of top tech giants, such as Microsoft, Oracle, Apache, and Apple. Also, there are some priority ones, for which the CISA has asked FCEB agencies to patch the vulnerabilities within February. Last month, the agency had warned federal agencies to fix old unpatched vulnerabilities.

Cyware News - Latest Cyber News

Emotet Malware Spreads by Hijacking Email Threats and Luring Users with Malicious Attachments
As early as December 21, 2021, researchers from Palo Alto Networks' Unit 42 observed a new infection method for the highly prevalent malware family Emotet involving thread hijacking.

Security Affairs

Experts disclose details of Apache Cassandra DB RCE
Researchers disclose a now-patched remote code execution (RCE) vulnerability in the Apache Cassandra database software. JFrog researchers publicly disclosed details of a now-patched high-severity security vulnerability (CVE-2021-44521) in Apache Cassandra database software that could be exploited by remote attackers to achieve code execution on affected installations. Apache Cassandra is an open-source NoSQL distributed database used [...] The post Experts disclose details of Apache Cassandra DB RCE appeared first on Security Affairs.

IT Security Guru

Google doubles bug bounties
Google has announced that they have doubled the rewards for anyone who can who can demonstrate working exploits for a range of zero-day and one-day vulnerabilities across a variety of platforms. The reward increases are applicable to exploits discovered in the Linux Kernel, Kubernetes, Google Kubernetes Engine (GKE), or kCTF (Kubernetes-based infrastructure for capture the [...] The post Google doubles bug bounties appeared first on IT Security Guru.

IT Security Guru

Hackers targeting people with fake Track and Trace texts
Scan text messages claiming to be from NHS Test and Trace have been circulating recently, Cornwall council warns. The messages falsely claim that the recipient has been in close contact with someone that has tested positive for Covid and asks them to click on a link to book a test. The texts are sent from [...] The post Hackers targeting people with fake Track and Trace texts appeared first on IT Security Guru.

ZDNet | security RSS

How the initial access broker market leads to ransomware attacks
Researchers explore the attack methods of LockBit, Avaddon, Darkside, Conti, and BlackByte ransomware groups.

IT Security Guru

### Lessons Learned From the 2022 NPM Corruption

Marak Squires is the maintainer of the 'colors' and 'faker' libraries. The two projects accumulate ~23 million weekly downloads and support ~23,000 projects. In January of 2022, he intentionally introduced an infinite loop that bricked every project relying on either one of these libraries. Consequently, GitHub suspended the developer's account. The justification provided by the [...] The post Lessons Learned From the 2022 NPM Corruption appeared first on IT Security Guru.

Cyware News - Latest Cyber News

### Log4Shell: A retrospective

An attacker could use this notorious vulnerability (dubbed Log4Shell) to force a victim to download, install and execute externally hosted malicious payloads with relative ease.

Threatpost

### Massive LinkedIn Phishing, Bot Attacks Feed on the Job-Hungry

The phishing attacks are spoofing LinkedIn to target 'Great Resignation' job hunters, who are also being preyed on by huge data-scraping bot attacks.

Cyware News - Latest Cyber News

### Missouri prosecutor declines to file charges over 'hacker' allegation against reporter

Missouri's public prosecutor has decided not to file charges against a journalist accused of illegal hacking over his disclosure of security vulnerabilities in a state government-run website.

The Hacker News

### Moses Staff Hackers Targeting Israeli Organizations for Cyber Espionage

The politically motivated Moses Staff hacker group has been observed using a custom multi-component toolset with the goal of carrying out espionage against its targets as part of a new campaign that exclusively singles out Israeli organizations. First publicly documented in late 2021, Moses Staff is believed to be sponsored by the Iranian government, with attacks reported against entities in

Cyware News - Latest Cyber News

### Nearly three-quarters of ransomware revenue generated by Russian strains

Nearly $3 in every $4 paid to a ransomware attack stems from a ransomware strain affiliated with Russian actors, according to a new report from cryptocurrency forensics group Chainalysis.

CyberScoop

### Red Cross attributes server breach to nation-state actor

The International Committee of the Red Cross has concluded that a nation-state hacker was behind a cyberattack on its servers discovered last month. A forensic analysis of the attack revealed the use of tools designed specifically to go after ICRC servers, the organization said Wednesday. "This was a sophisticated attack -- a criminal act -- breaching sensitive humanitarian data," ICRC Director-General Robert Mardini said. "We know that the attack was targeted because the attackers created code designed solely for execution on the concerned ICRC servers, a technique we believe was designed to shield the hackers' activities from detection and subsequent forensic investigations." Separate from[...]

The Hacker News

### Researchers Warn of a New Golang-based Botnet Under Continuous Development

Cybersecurity researchers have unpacked a new Golang-based botnet called Kraken that's under active development and features an array of backdoor capabilities to siphon sensitive information from compromised Windows hosts. "Kraken already features the ability to download and execute secondary payloads, run shell commands, and take screenshots of the victim's system," threat intelligence firm

Cyware News - Latest Cyber News

### Singapore introduces strong measures to stop online scams

Singapore will step up up efforts to stamp out phishing and spoofing, ministers told the parliament on Tuesday. The topic gained attention after instances of attacks and scams soared recently.

The Hacker News

### This New Tool Can Retrieve Pixelated Text from Redacted Documents

The practice of blurring out text using a method called pixelation may not be as secure as previously thought. While the most foolproof way of concealing sensitive textual information is to use opaque black bars, other redaction methods like pixelation can achieve the opposite effect, enabling the reversal of pixelized text back into its original form. Dan Petro, a lead researcher at offensive

IT Security Guru

### Trickbot hits top brands, attacks customers

Trickbot, the bane of many cybersecurity professionals lives', has begun to target the customers of 60 major institutions including Wells Fargo and Bank of America. The attacks come through web injections and phishing campaigns. Initially, Trickbot was a relatively simple Banking Trojan similar to Zeus, Agent Tesla, Dridex and DanaBot. Following the retirement of the [...] The post Trickbot hits top brands, attacks customers appeared first on IT Security Guru.

Threatpost

### TrickBot Ravages Customers of Amazon, PayPal and Other Top Brands

The resurgent trojan has targeted 60 top companies to harvest credentials for a wide range of applications, with an eye to virulent follow-on attacks.

Cyware News - Latest Cyber News

### LinkedIn phishing scams increase 232% since Feb 1: report

Cybercriminals are using display name spoofing and stylized HTML templates to lure victims into clicking on phishing links in Outlook 365 and then entering their credentials into fraudulent websites.

IT Security Guru

### Major Canadian banks go offline in unexplained outage

The mysterious outage is as yet unexplained and hit Royal Bank of Canada (RBC), Bank of Montreal (BMO), Scotiabank, TD Bank Canada and the Canadian Imperial Bank of Commerce (CIBC). "We are currently experiencing technical issues with our online and mobile banking, as well as our phone systems," an RBC representative confirmed. "Our experts are investigating [...] The post Major Canadian banks go offline in unexplained outage appeared first on IT Security Guru.

Cyware News - Latest Cyber News

### Meet Kraken: A New Golang Botnet in Development

Since October 2021, ZeroFox Intelligence researchers have been tracking Kraken - a previously unknown botnet targeting Windows that is currently under active development.

ZDNet | security RSS

### Missouri will not prosecute 'hacker' reporter for daring to view state website HTML

Missouri's governor was both criticized and mocked for saying the journalist "decoded HTML source code" for malicious purposes.

Security Affairs

### Nation-state actors hacked Red Cross exploiting a Zoho bug

The International Committee of the Red Cross (ICRC) said attackers that breached its network last month exploited a Zoho bug. The International Committee of the Red Cross (ICRC) revealed that the attack that breached its network in January was conducted by a nation-state actor that exploited a Zoho vulnerability. In January, a cyberattack on a [...] The post Nation-state actors hacked Red Cross exploiting a Zoho bug appeared first on Security Affairs.

Security Affairs

### New Kraken botnet is allowing operators to earn USD 3,000 every month

Researchers spotted a new Golang-based botnet called Kraken that is under active development and supports a lot of backdoor capabilities. Kraken is a new Golang-based botnet discovered in late October 2021 by researchers from threat intelligence firm ZeroFox Intelligence. Experts pointed out that despite having the same name, this botnet should not be confused with the Kraken [...] The post New Kraken botnet is allowing operators to earn USD 3,000 every month appeared first on Security Affairs.

Krebs on Security

### Red Cross Hack Linked to Iranian Influence Operation?

A network intrusion at the International Committee for the Red Cross (ICRC) in January led to the theft of personal information on more than 500,000 people receiving assistance from the group. KrebsOnSecurity has learned that the email address used by a cybercriminal actor who offered to sell the stolen ICRC data also was used to register multiple domain names the FBI says are tied to a sprawling media influence operation originating from Iran.

Security Affairs

### Russia-linked threat actors breached US cleared defense contractors (CDCs)

Russia-linked threat actors have breached the network of U.S. cleared defense contractors (CDCs) since at least January 2020. According to a joint alert published by the FBI, NSA, and CISA, Russia-linked threat actors conducted a cyber espionage campaign aimed at US cleared defense contractors to steal sensitive info related to intelligence programs and capabilities. CDCs [...] The post Russia-linked threat actors breached US cleared defense contractors (CDCs) appeared first on Security Affairs.

Cyware News - Latest Cyber News

### Supply chain shortages create a cybersecurity nightmare

Supply chain issues are already one of the weakest links for an organization, even in the best of times. Challenges are not just in production capabilities, but also in security of the final product.

ZDNet | security RSS

### Trickbot abuses top brands including Bank of America, Wells Fargo in attacks against customers

The malware is said to pose a "great danger" to the customers of 60 finance and tech giants.

The Hacker News

### Trickbot Malware Targeted Customers of 60 High-Profile Companies Since 2020

The notorious TrickBot malware is targeting customers of 60 financial and technology companies, including cryptocurrency firms, primarily located in the U.S., even as its operators have updated the botnet with new anti-analysis features. "TrickBot is a sophisticated and versatile malware with more than 20 modules that can be downloaded and executed on demand," Check Point researchers Aliaksandr

Security Affairs

### Trickbot targets customers of 60 High-Profile companies

TrickBot malware is targeting customers of 60 financial and technology companies with new anti-analysis features. The infamous TrickBot malware was employed in attacks against customers of 60 financial and technology companies with new anti-analysis features. The news wave of attacks aimed at cryptocurrency firms, most of them located in the U.S.. Trickbot is a sophisticated, [...] The post Trickbot targets customers of 60 High-Profile companies appeared first on Security Affairs.

The Hacker News

U.S. Says Russian Hackers Stealing Sensitive Data from Defense Contractors

State-sponsored actors backed by the Russian government regularly targeted the networks of several U.S. cleared defense contractors (CDCs) to acquire proprietary documents and other confidential information pertaining to the country's defense and intelligence programs and capabilities. The sustained espionage campaign is said to have commenced at least two years ago from January 2020, according

Cyware News - Latest Cyber News

US Postal Service emergency records system will expand to support ransomware, breach response

The agency claims that paper and electronic records for the system are located in "controlled-access areas" and under supervision to limit access to authorized personnel.

The Hacker News

VMware Issues Security Patches for High-Severity Flaws Affecting Multiple Products

VMware on Tuesday patched several high-severity vulnerabilities impacting ESXi, Workstation, Fusion, Cloud Foundation, and NSX Data Center for vSphere that could be exploited to execute arbitrary code and cause a denial-of-service (DoS) condition. As of writing, there's no evidence that any of the weaknesses are exploited in the wild. The list of six flaws is as follows -

CyberScoop

Website disruptions were attempt to sow discord and cause panic, Ukraine officials say

Tuesday's disruption of multiple Ukrainian government websites and web services for several state-owned banks -- along with spam text messages falsely claiming ATMs didn't work -- were part of a coordinated operation designed to sow panic, Ukrainian government officials claimed Wednesday. The officials said it was "too early to talk about specific actors" associated with the distributed denial-of-service (DDoS) attacks, but that the targeting of multiple websites, along with the text messages, suggested an extensive effort beyond the range of an individual or even a group of hackers. The remarks, from some of Ukraine's cybersecurity and law enforcement leaders, came at a joint briefing Wedne[...]

Cyware News - Latest Cyber News

US Agencies Warn of Russian Cyber Activity Targeting Cleared Defense Contractors

Over the last two years, compromised entities have included cleared defense contractors supporting the U.S. Army, U.S. Air Force, U.S. Navy, U.S. Space Force, and Intelligence Community programs.

Naked Security

VMWare fixes holes that could allow virtual machine escapes

Hats off to VMWare for not using weasel words: "When should you act?" Immediately...

Cyware News - Latest Cyber News

Vulnerability spotted in Hancom Office could lead to memory corruption, code execution

Cisco Talos recently discovered a flaw in Hancom Office -- a popular software suite in South Korea -- that could allow an attacker to corrupt memory on the targeted machine or execute remote code.

## Twitter

RedPacket Security

HUAWEI EMUI/Magic UI code execution | CVE-2021-39994 -

CVE

CVE-2021-39994 There is an arbitrary address access vulnerability with the product line test code.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.

Wolfgang Sesin

New post from (CVE-2021-39997) has been published on

www.sesin.at

New post from (Huawei EMUI Audio out-of-bounds read [CVE-2021-39997]) has been published on

Threat Intel Center

NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

Remotely Alerts

Severity: | There is a vulnerability of unstrict inp... | CVE-2021-39997 | Link for more:

RedPacket Security

HUAWEI EMUI/Magic UI code execution | CVE-2021-39997 -

CVE

CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access.

www.sesin.at

New post from (CVE-2021-39997) has been published on

Wolfgang Sesin

New post from (Huawei EMUI Audio out-of-bounds read [CVE-2021-39997]) has been published on

Threat Intel Center

NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

Threat Intel Center

NEW: CVE-2021-39997 There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access. Severity: CRITICAL

*Source: NIST*

## NIST CVE: Critical

CVE-2021-45364

A Code Execution vulnerability exists in **Statamic** Version through 3.2.26 via SettingsController.php.

CRITICAL Vector: network Created: 2022-02-10 Updated: 2022-02-17

CVE-2022-24310

A CWE-190: Integer Overflow or Wraparound vulnerability exists that could cause heap-based buffer overflow, leading to denial of service and potentially remote code execution when an attacker sends multiple specially crafted messages. Affected Product: **Interactive Graphical SCADA System** Data Server (V15.0.0.22020 and prior)

CRITICAL Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-24311

A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause modification of an existing file by inserting at beginning of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: **Interactive Graphical SCADA System** Data Server (V15.0.0.22020 and prior)

CVE-2022-24313

A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could cause a stack-based buffer overflow potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: **Interactive Graphical SCADA System** Data Server (V15.0.0.22020 and prior)

CRITICAL Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-24312

A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause modification of an existing file by adding at end of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: **Interactive Graphical SCADA System** Data Server (V15.0.0.22020 and prior)

CRITICAL Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-20738

A vulnerability in the **Cisco Umbrella Secure Web Gateway** service could allow an unauthenticated, remote attacker to bypass the file inspection feature. This vulnerability is due to insufficient restrictions in the file inspection feature. An attacker could exploit this vulnerability by downloading a crafted payload through specific methods. A successful exploit could allow the attacker to bypass file inspection protections and download a malicious payload.

CRITICAL Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-24954

**Foxit PDF Reader** before 11.2.1 and Foxit PDF Editor before 11.2.1 have a Stack-Based Buffer Overflow related to XFA, for the 'subform colSpan="-2"' and 'draw colSpan="1"' substrings.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-17

CVE-2022-24568

Novel-plus v3.6.0 was discovered to be vulnerable to Server-Side Request Forgery (SSRF) via user-supplied crafted input.

CRITICAL Vector: network Created: 2022-02-10 Updated: 2022-02-17

CRITICAL Vector: network Created: 2022-02-10 Updated: 2022-02-17

CVE-2022-24955

**Foxit PDF Reader** before 11.2.1 and Foxit PDF Editor before 11.2.1 have an Uncontrolled Search Path Element for DLL files.

CRITICAL Vector: network Created: 2022-02-11 Updated: 2022-02-17

*Source: NIST*

## NIST CVE: High

CVE-2022-24318

A CWE-326: Inadequate Encryption Strength vulnerability exists that could cause non-encrypted communication with the server when outdated versions of the ViewX client are used. Affected Product: **ClearSCADA** (All Versions), **EcoStruxure Geo SCADA Expert 2019** (All Versions), **EcoStruxure Geo SCADA Expert 2020** (All Versions)

HIGH Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-23773

cmd/go in Go before 1.16.14 and 1.17.x before 1.17.7 can misinterpret branch names that falsely appear to be version tags. This can lead to incorrect access control if an actor is supposed to be able to create branches but not tags.

HIGH Vector: network Created: 2022-02-11 Updated: 2022-02-17

CVE-2022-23048

**Exponent CMS** 2.6.0patch2 allows an authenticated admin user to upload a malicious extension in the format of a ZIP file with a PHP file inside it. After upload it, the PHP file will be placed at "themes/simpletheme/{rce}.php" from where can be accessed in order to execute commands.

HIGH Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-23772

Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Memory Consumption.

HIGH Vector: network Created: 2022-02-11 Updated: 2022-02-17

CVE-2022-24317

A CWE-862: Missing Authorization vulnerability exists that could cause information exposure when an attacker sends a specific message. Affected Product: **Interactive Graphical SCADA System** Data Server (V15.0.0.22020 and prior)

HIGH Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-24647

Cuppa CMS v1.0 was discovered to contain an arbitrary file deletion vulnerability via the unlink() function.

HIGH Vector: network Created: 2022-02-10 Updated: 2022-02-17

CVE-2022-24646

**Hospital Management System** v4.0 was discovered to contain a SQL injection vulnerability in /Hospital-Management-System-master/contact.php via the txtMsg parameters.

HIGH Vector: network Created: 2022-02-10 Updated: 2022-02-17

*Source: NIST*

## NIST CVE: Medium

CVE-2022-23321

A persistent cross-site scripting (XSS) vulnerability exists on two input fields within the administrative panel when editing users in the XMPie UStore application on version 12.3.7244.0.

MEDIUM Vector: network Created: 2022-02-10 Updated: 2022-02-17

CVE-2022-23628

OPA is an open source, general-purpose policy engine. Under certain conditions, pretty-printing an abstract syntax tree (AST) that contains synthetic nodes could change the logic of some statements by reordering array literals. Example of policies impacted are those that parse and compare web paths. **All of these** **three** conditions have to be met to create an adverse effect: 1. An AST of Rego had to be **created programmatically** such that it ends up containing terms without a location (such as wildcard variables). 2. The AST had to be **pretty-printed** using the `github.com/open-policy-agent/opa/format` package. 3. The result of the pretty-printing had to be **parsed and evaluated again** via an OPA instance using the bundles, or the **Golang** packages. If any of these three conditions are not met, you are not affected. Notably, all three would be true if using **optimized bundles**, i.e. bundles created with `opa build -O=1` or higher. In that case, the optimizer would fulfil condition (1.), the result of that would be pretty-printed when writing the bundle to disk, fulfilling (2.). When the bundle was then used, we'd satisfy (3.). As a workaround users may disable optimization when creating bundles.

MEDIUM Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-23049

**Exponent CMS** 2.6.0patch2 allows an authenticated user to inject persistent JavaScript code on the "User-Agent" header when logging in. When an administrator user visits the "User Sessions" tab, the JavaScript will be triggered allowing an attacker to compromise the administrator session.

MEDIUM Vector: network Created: 2022-02-09 Updated: 2022-02-17

CVE-2022-22780

The **Zoom** Client for **Meetings** chat functionality was susceptible to Zip bombing attacks in the following product versions: **Android** before version 5.8.6, iOS before version 5.9.0, **Linux** before version 5.8.6, **macOS** before version 5.7.3, and **Windows** before version 5.6.3. This could lead to availability issues on the client host by exhausting system **resources**.

MEDIUM Vector: network Created: 2022-02-09 Updated: 2022-02-17

*Source: NIST*

## NIST CVE: Low

***Nothing today***

*Source: NIST*

## NIST CVE: Unrated

CVE-2022-0622

Generation of Error Message Containing Sensitive Information in Packagist snipe/snipe-it prior to 5.3.11.

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-17

CVE-2022-0623

Out-of-bounds Read in Homebrew **mruby** prior to 3.2.

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-17

CVE-2022-0572

Heap-based Buffer Overflow in **GitHub** repository vim/vim prior to 8.2.

UNRATED Vector: unkown Created: 2022-02-14 Updated: 2022-02-17

CVE-2022-24953

The Crypt_GPG extension before 1.6.7 for PHP does not prevent additional options in GPG calls, which presents a risk for certain environments and GPG versions.

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-17

CVE-2022-25270

The **Quick Edit** module does not properly check entity access in some circumstances. This could result in users with the "access in-place editing" permission viewing some content they are are not authorized to access. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed.

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-17

CVE-2022-22901

There is an Assertion in 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at parser_parse_function_arguments in /js/js-parser.c of **JerryScript** commit a6ab5e9.

UNRATED Vector: unkown Created: 2022-02-17 Updated: 2022-02-17

*Source: Hybrid Analysis*

## Top malicious files

| | |
|---|---|
| 100%<br>Threat score | M5_Game_v3 (.) exe |
| 100%<br>Threat score | CM-696532968 (.) xlsb |
| 100%<br>Threat score | W7XGpodRs5kYvnV |
| 100%<br>Threat score | MoChat (.) apk |
| 100%<br>Threat score | MK-41 (.) exe |
| 100%<br>Threat score | suallar (.) scr |
| 100%<br>Threat score | New RFQ Oder List Scg,pdf (.) ppam |
| 95%<br>Threat score | MedWin (.) xls |
| 74%<br>Threat score | ZoneAlarm Mobile Security & Antivirus Protection v1 (.) 78-2411 Premium [FileCR] (.) apk |
| 100%<br>Threat score | v_MULTI_MIX_nosleep_5e244bf3a2fe36942e9e001bbb6677f6c8e2dbbd1d74f74a8d0cb9f78c9e4a57_0 (.) exe |
| 100%<br>Threat score | REFS_45015 (.) exe |
| 100%<br>Threat score | ratnik (.) exe |
| 100%<br>Threat score | ads4-Spanien-1 (.) 16 (.) 0 (.) 7-setup (.) exe |
| 100%<br>Threat score | Revealer (.) exe |
| 100%<br>Threat score | fastxp (.) exe (.) noexec |
| 97%<br>Threat score | 9faa1e0ec64017af9d2ec7a844046ea3baf425de027afc3bd100712f377a9570 (.) xlsx |
| 95%<br>Threat score | v_MULTI_MIX_nosleep_413ebd37620cfcb229322a0f3217ae8a6a61163eb73b14a30e3d8d5a68847f1b_0 (.) exe |

*Source: Hybrid Analysis*

## Top malicious URL

| | |
|---|---|
| 100%<br>Threat score | http://quetzalgt (.) coffee/images/B5WUc/ |
| 100%<br>Threat score | http://mailupdatenavybdzimbra (.) gov-pk (.) org/ |
| 100%<br>Threat score | http://edinsonjhernandez (.) info/wp-content/BaazJljahSR2/ |
| 100%<br>Threat score | http://pakcert (.) gov-pk (.) org/zaqxswcde (.) hta (.) |
| 95%<br>Threat score | http://xn--80apgfhelckg6l (.) xn--p1ai/ |
| 95%<br>Threat score | http://mfamailzimbraupdation (.) gov-pk (.) org/ |
| 90%<br>Threat score | http://pakcert (.) gov-pk (.) org/zaqxswcderfv (.) hta: |
| 81%<br>Threat score | https://stayathomeamerica (.) com/wp-content/nrQWW/ |
| 78%<br>Threat score | http://sanlorenzoyacht (.) com:443/newsl/include/inc-map (.) asp |
| 77%<br>Threat score | http://tagisebutt (.) ga/user/117935 |
| 77%<br>Threat score | https://nam10 (.) safelinks (.) protection (.) outlook (.) com/?url=https%3A%2F%2Furldefense (.) proofpoint (.) com%2Fv2%2Furl%3Fu%3Dhttps-3A__nam10 (.) safelinks (.) protection<br>(.) com-257C6be74e77b36c4764f26708d9ec9bb688-257Ce6f978e175d44db0904e5b79fb778570-257C0-257C0-257C637800976264165292-257CUnknown-257CTWFpbGZsb3d8eyJW<br>252BGHO1hBs2Qf-252FvIoILhU-253D-26reserved-3D0%26d%3DDwMFAg%26c%3DudBTRvFvXC5Dhqg7UHpJlPps3mZ3LRxpb6__0PomBTQ%26r%3Dh6aC2jAuvZlppNAHAp9XyAJPK<br>NHogJz2M0_W09Fq3f8aLTCJVRn%26s%3DUcMUUCXM6FxC1gwwNFD3AzAiiLK7ZE9c0QIbUSwqEyU%26e%3D&data=04%7C01%7Ctania (.) parmar%40johnsonfleming (.)<br>com%7C8aebf866702345df376d08d9ecc8de06%7Ce6f978e175d44db0904e5b79fb778570%7C0%7C0%7C637801169760294807%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjA |
| 72%<br>Threat score | http://docdrag (.) com/ |

*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 Japan
- #9 Brazil
- #10 Korea, Republic of

*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 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#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 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#7 **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.

#8 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#9 **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.

*Source: SpamHaus*

## Top countries with botnet

- #1 China
- #2 India
- #3 United States of America
- #4 Thailand
- #5 Indonesia
- #6 Algeria
- #7 Viet Nam
- #8 Brazil
- #9 Iran (Islamic Republic of)
- #10 Pakistan

*Source: SpamHaus*

## Top phishing countries

- #1 United States
- #2 Germany
- #3 Russia
- #4 Netherlands
- #5 France
- #6 Hong Kong
- #7 Singapore
- #8 United Kingdom
- #9 Finland
- #10 India