



Ausgabe: 20230823

Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

Security-News

Heise - Security-Alert

Sicherheitslücken: Smarte Glühbirne von TP-Link als Einfallstor ins WLAN

Sicherheitsforscher warnen in einem wissenschaftlichen Artikel welche Gefahr selbst von vergleichsweise simplen IoT-Geräten ausgehen kann.

- [Link](#)

Jetzt patchen! Angreifer schieben Schadcode durch Lücke in Adobe ColdFusion

Angreifer attackieren Adobes Middleware ColdFusion. Sicherheitsupdates sind verfügbar.

- [Link](#)

Kritische Sicherheitslücke in Ivanti Sentry wird bereits missbraucht

Ivanti schließt in Sentry, vormals MobileIron Sentry, eine kritische Sicherheitslücke. Sie wird bereits angegriffen.

- [Link](#)

Angreifer können Sicherheitslücken in Junos OS zu kritischer Gefahr eskalieren

Das Netzwerkbetriebssystem Junos OS ist über mehrere Schwachstellen attackierbar. Dagegen abgesicherte Versionen stehen zum Download bereit.

- [Link](#)

Update bereits ausgespielt: Kritische Lücke in WinRAR erlaubt Code-Ausführung

Das verbreitete Kompressionstool WinRAR besaß in älteren Versionen eine schwere Lücke, die beliebige Codeausführung erlaubte. Die aktuelle Version schließt sie.

- [Link](#)

Sicherheitslösung: IBM Security Guardium als Einfallstor für Angreifer

Eine kritische Lücke bedroht Systeme mit IBM Security Guardium. Sicherheitspatches sind verfügbar.

- [Link](#)

Sicherheitsupdates: Root-Lücken bedrohen Cisco-Produkte

Es sind wichtige Sicherheitsupdates für unter anderem Cisco Unified Communications Manager und Prime Infrastructure erschienen.

- [Link](#)

Jetzt patchen! Citrix ShareFile im Visier von Angreifern

Unbekannte Angreifer nutzen eine kritische Sicherheitslücke in Citrix ShareFile StorageZones Controller aus. Updates sind verfügbar.

- [Link](#)

Lücken in Kennzeichenerkennungssoftware gefährden Axis-Überwachungskamera

Mehrere Sicherheitslücken in Software für Überwachungskameras von Axis gefährden Geräte.

- [Link](#)

Sicherheitslücken: Angreifer können Hintertüren in Datenzentren platzieren

Schwachstellen in Software von CyberPower und Dataprobe zur Energieüberwachung und -Verteilung gefährden Datenzentren.

- [Link](#)

Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-39143	0.921370000	0.985580000	Link
CVE-2023-3519	0.911990000	0.984730000	Link
CVE-2023-35078	0.965240000	0.994120000	Link
CVE-2023-34362	0.936790000	0.987620000	Link
CVE-2023-33246	0.963860000	0.993550000	Link
CVE-2023-28771	0.918810000	0.985340000	Link
CVE-2023-28121	0.937820000	0.987720000	Link
CVE-2023-27372	0.970840000	0.996600000	Link
CVE-2023-27350	0.971160000	0.996780000	Link
CVE-2023-25717	0.967140000	0.994960000	Link
CVE-2023-25194	0.924830000	0.985930000	Link
CVE-2023-24489	0.967300000	0.995040000	Link
CVE-2023-21839	0.961530000	0.992820000	Link
CVE-2023-21554	0.902620000	0.983880000	Link
CVE-2023-20887	0.960660000	0.992600000	Link
CVE-2023-0669	0.965780000	0.994390000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 22 Aug 2023

[UPDATE] [kritisch] Python: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 22 Aug 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Tue, 22 Aug 2023

[UPDATE] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 22 Aug 2023

[NEU] [hoch] Ivanti Sentry: Schwachstelle ermöglicht Umgehung von Sicherheitsmechanismen

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Ivanti Sentry ausnutzen, um Sicherheitsmechanismen zu umgehen.

- [Link](#)

Mon, 21 Aug 2023

[NEU] [hoch] Moodle: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um Sicherheitsmechanismen zu umgehen, Informationen offenzulegen und SQL-Injection- oder Cross-Site-Scripting-Angriffe durchzuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Schwachstelle ermöglicht Denial-of-Service

Ein entfernter, anonym Angreifer kann eine Schwachstelle in vim ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Speicher zu verändern und möglicherweise beliebigen Code auszuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen und einen Denial of Service zu verursachen oder Daten zu manipulieren oder offenzulegen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und einen Denial-of-Service-Zustand zu verursachen

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, Speicher zu manipulieren und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] Mozilla Firefox und Mozilla Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Mon, 21 Aug 2023

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

Mon, 21 Aug 2023

[NEU] [hoch] genua genucenter: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in genua genucenter ausnutzen, um Informationen offenzulegen, Dateien zu manipulieren, um Cross-Site Scripting Angriffe durchzuführen oder um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/22/2023	[Debian DSA-5481-1 : fastdds - security update]	critical
8/22/2023	[Citrix ShareFile Documents Unauthenticated Access (CTX559517)]	critical
8/22/2023	[Fedora 38 : GitPython (2023-1ec4e542f9)]	critical
8/22/2023	[Debian DLA-3538-1 : zabbix - LTS security update]	critical

Datum	Schwachstelle	Bewertung
8/21/2023	[openSUSE 15 Security Update : python-mitmproxy (openSUSE-SU-2023:0233-1)]	critical
8/21/2023	[openSUSE 15 Security Update : python-mitmproxy (openSUSE-SU-2023:0232-1)]	critical
8/20/2023	[Fedora 38 : chromium (2023-f8e94641dc)]	critical
8/19/2023	[SUSE SLES12 Security Update : nodejs16 (SUSE-SU-2023:3355-1)]	critical
8/22/2023	[openSUSE 15 Security Update : chromium (openSUSE-SU-2023:0234-1)]	high
8/22/2023	[Fedora 38 : clamav (2023-bf72d8833e)]	high
8/22/2023	[QNAP QTS / QuTS hero DoS (QSA-23-09)]	high
8/22/2023	[Debian DSA-5480-1 : linux - security update]	high
8/22/2023	[Debian DLA-3536-1 : flask - LTS security update]	high
8/22/2023	[RHEL 7 : kernel (RHSA-2023:4697)]	high
8/22/2023	[Fedora 37 : linux-firmware (2023-eabbf4ca4d)]	high
8/22/2023	[Fedora 37 : java-17-openjdk (2023-9ef4ec10da)]	high
8/22/2023	[Fedora 38 : python-yfinance (2023-2b0f2e4bc3)]	high
8/22/2023	[RHEL 7 : kernel (RHSA-2023:4699)]	high
8/22/2023	[RHEL 7 : kernel (RHSA-2023:4696)]	high
8/22/2023	[RHEL 7 : kpatch-patch (RHSA-2023:4698)]	high
8/22/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Inetutils vulnerabilities (USN-6304-1)]	high
8/22/2023	[RHEL 8 : subscription-manager (RHSA-2023:4706)]	high
8/22/2023	[RHEL 8 : subscription-manager (RHSA-2023:4703)]	high
8/22/2023	[RHEL 8 : subscription-manager (RHSA-2023:4704)]	high
8/22/2023	[RHEL 9 : subscription-manager (RHSA-2023:4708)]	high
8/22/2023	[RHEL 8 : subscription-manager (RHSA-2023:4705)]	high
8/22/2023	[RHEL 9 : subscription-manager (RHSA-2023:4707)]	high
8/22/2023	[RHEL 7 : subscription-manager (RHSA-2023:4701)]	high
8/22/2023	[RHEL 8 : subscription-manager (RHSA-2023:4702)]	high
8/21/2023	[Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS : Vim vulnerabilities (USN-6302-1)]	high
8/21/2023	[Jenkins plugins Multiple Vulnerabilities (2023-08-16)]	high
8/21/2023	[Security Updates for Microsoft SQL Server ODBC Driver (August 2023)]	high
8/21/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : ClamAV vulnerability (USN-6303-1)]	high
8/21/2023	[F5 Networks BIG-IP : Python urllib.parse vulnerability (K000135921)]	high
8/21/2023	[Ubuntu 16.04 ESM / 18.04 ESM : ClamAV vulnerability (USN-6303-2)]	high
8/21/2023	[Rockwell Automation PowerMonitor 1000 Improper Neutralization of Input During Web Page Generation (Cross-Site Scripting) (CVE-2023-2072)]	high
8/20/2023	[Fedora 37 : libreswan (2023-dbc6d8a124)]	high
8/20/2023	[Fedora 38 : libreswan (2023-ddd6e6b49b)]	high
8/20/2023	[Fedora 38 : dotnet6.0 / dotnet7.0 (2023-cbc688b8ca)]	high
8/20/2023	[Fedora 37 : dotnet6.0 / dotnet7.0 (2023-25112489ab)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Tue, 22 Aug 2023

WordPress Charitable Donations Plugin And Fundraising Platform 1.7.0.12 Privilege Escalation
WordPress Charitable Donations Plugin and Fundraising Platform versions 1.7.0.12 and below suffer from a privilege escalation vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

TSPPlus 16.0.2.14 Insecure Permissions

TSPPlus version 16.0.2.14 suffers from an insecure permissions vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

TSPPlus 16.0.0.0 Insecure Permissions

TSPPlus version 16.0.0.0 suffers from an insecure permissions vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

TSPPlus 16.0.0.0 Insecure Credential Storage

TSPPlus version 16.0.0.0 suffers from an insecure credential storage vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

Inosoft VisiWin 7 2022-2.1 Insecure Permissions / Privilege Escalation

Inosoft VisiWin 7 version 2022-2.1 suffers from a privilege escalation vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

Dolibarr 17.0.1 Cross Site Scripting

Dolibarr version 17.0.1 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

PHPJabbers Business Directory Script 3.2 Cross Site Request Forgery / Cross Site Scripting

PHPJabbers Business Directory Script version 3.2 suffers from cross site request forgery and cross site scripting vulnerabilities.

- [Link](#)

” “Tue, 22 Aug 2023

FOG Forum 0.8 Cross Site Scripting

FOG Forum version 0.8 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

FoccusWeb CMS 0.1 Cross Site Scripting

FoccusWeb CMS version 0.1 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

Fluent CMS 1.0.0 SQL Injection

Fluent CMS version 1.0.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

” “Tue, 22 Aug 2023

Color Prediction Game 1.0 SQL Injection

Color Prediction Game version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

Global Multi School Management System Express 1.0 SQL Injection

Global Multi School Management System Express version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

OVOO Movie Portal CMS 3.3.3 SQL Injection

OVOO Movie Portal CMS version 3.3.3 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

Taskhub CRM Tool 2.8.6 SQL Injection

Taskhub CRM Tool version 2.8.6 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

FlightPath LMS 4.8.2 Insecure Direct Object Reference

FlightPath LMS version 4.8.2 suffers from an insecure direct object reference vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

FleetCart Laravel Ecommerce System 1.1.2 Insecure Settings

FleetCart Laravel Ecommerce System version 1.1.2 suffers from an ignored default credential vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

FixBook Repair Shop Management Tool 2.2 Hash Disclosure

FixBook Repair Shop Management Tool version 2.2 suffers from an information leakage vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

DoorGets CMS 12 Information Disclosure

DoorGets CMS version 12 suffers from an information leakage vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

FIRESHOP Advanced CMS 2.3 Arbitrary File Upload

FIRESHOP Advanced CMS version 2.3 suffers from an arbitrary file upload vulnerability.

- [Link](#)

” “Tue, 22 Aug 2023

FastMatch Iddaa Tahmin Scripti 2.0 SQL Injection

FastMatch Iddaa Tahmin Scripti version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

” “Tue, 22 Aug 2023

E-mailer Newsletter And Mailing System with Analytics + GEO location 1.16 Information Disclosure

E-mailer Newsletter and Mailing System with Analytics + GEO location version 1.16 suffers from an information leakage vulnerability.

- [Link](#)

” “Mon, 21 Aug 2023

Jorani Remote Code Execution

This Metasploit module exploits an unauthenticated remote code execution vulnerability in Jorani versions prior to 1.0.2. It abuses log poisoning and redirection bypass via header spoofing and then it uses path traversal to trigger the vulnerability. It has been tested on Jorani 1.0.0.

- [Link](#)

” “Mon, 21 Aug 2023

Academy LMS 6.1 Cross Site Scripting / File Upload

Academy LMS version 6.1 suffers from an upload vulnerability that could lead to persistent cross site scripting attacks.

- [Link](#)

” “Mon, 21 Aug 2023

Credit Lite 1.5.4 SQL Injection

Credit Lite version 1.5.4 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Mon, 21 Aug 2023

Crypto Currency Tracker (CCT) 9.5 Add Administrator

Crypto Currency Tracker (CCT) versions 9.5 and below suffer from a flaw that allows an administrative account to be added without authentication.

- [Link](#)

”

0-Day

“Tue, 22 Aug 2023

ZDI-23-1163: NETGEAR RAX30 Telnet CLI passwd Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Tue, 22 Aug 2023

ZDI-23-1162: NETGEAR RAX30 DHCP Server Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Tue, 22 Aug 2023

ZDI-23-1161: NETGEAR RAX30 UPnP Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Tue, 22 Aug 2023

ZDI-23-1160: Parse Server transformUpdate Prototype Pollution Remote Code Execution Vulnerability

- [Link](#)

” “Tue, 22 Aug 2023

ZDI-23-1159: Apple macOS KTX Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Mon, 21 Aug 2023

ZDI-23-1158: McAfee Safe Connect VPN Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

- [Link](#)

” “Mon, 21 Aug 2023

ZDI-23-1157: Advantech R-SeeNet device__status Local File Inclusion Privilege Escalation Vulnerability

- [Link](#)

” “Mon, 21 Aug 2023

ZDI-23-1156: Advantech R-SeeNet Use Of Hard-Coded Credentials Authentication Bypass Vulnerability

- [Link](#)

” “Mon, 21 Aug 2023

ZDI-23-1155: SonicWALL GMS Virtual Appliance HttpDigestAuthenticator Authentication Bypass Vulnerability

- [Link](#)

” “Mon, 21 Aug 2023

ZDI-23-1154: SonicWALL GMS Virtual Appliance Syslog Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 21 Aug 2023

ZDI-23-1153: 3CX Uncontrolled Search Path Local Privilege Escalation Vulnerability

- [Link](#)

”

Die Hacks der Woche

mit Martin Haunschmid

Wasser predigen und Wein trinken? Ivanti, als Security Hersteller DARF so etwas nicht passieren!



[Zum Youtube Video](#)

Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2023-08-21	Hôpital municipal Sfânta Treime de Chişinău	[MDA]	Link
2023-08-21	Le Centre Public d'Action Sociale (CPAS) de Charleroi	[BEL]	Link
2023-08-20	Kansai Nerolac Ltd.	[IND]	Link
2023-08-20	Singing River Health System	[USA]	Link
2023-08-18	Energy One Limited	[AUS]	Link
2023-08-17	Poste Italiane	[ITA]	Link
2023-08-17	La mairie de Sartrouville	[FRA]	Link
2023-08-16	Le consortium de bonification de l'Emilia Centrale	[ITA]	Link
2023-08-15	Cleveland City Schools	[USA]	Link
2023-08-14	Clorox	[USA]	Link
2023-08-14	Prince George's County Public Schools	[USA]	Link
2023-08-13	Swan Retail	[GBR]	Link
2023-08-13	Verlagsgruppe in München	[DEU]	Link
2023-08-11	Neogy	[ITA]	Link
2023-08-11	Freeport-McMoRan Inc.	[USA]	Link
2023-08-09	Rapattoni	[USA]	Link
2023-08-08	Fondation de Verdeil	[CHE]	Link
2023-08-07	Centre médical Mayanei Hayeshua	[ISR]	Link
2023-08-07	Oniris	[FRA]	Link
2023-08-06	Le Service de Santé de Madeira (Sesaram)	[PRT]	Link
2023-08-04	Trinkwasserverband (TWV) Stader Land	[DEU]	Link
2023-08-03	Prospect Medical Holdings	[USA]	Link
2023-08-03	Commission des services électriques de Montréal (CSEM)	[CAN]	Link
2023-08-02	BPP	[GBR]	Link
2023-08-02	Joyson Safety Systems	[DEU]	Link
2023-08-02	L'Association du Barreau Fédéral Allemand (BRAK)	[DEU]	Link
2023-08-01	Programme de Soins Médicaux Intégrés (PAMI)	[ARG]	Link
2023-08-01	Eastern Connecticut Health Network (ECHN) et Waterbury HEALTH	[USA]	Link
2023-08-01	NOIRLab	[USA]	Link

Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-22	[A???? F????????? Ltd]	play	Link
2023-08-22	[tonystark.com]	lockbit3	Link
2023-08-22	[Sirius Computer Solutions]	alphv	Link
2023-08-22	[Atlantic Federal Credit Union]	alphv	Link
2023-08-22	[decrolyamericano.edu.gt]	lockbit3	Link
2023-08-22	[sicl.lk]	lockbit3	Link
2023-08-22	[NE-BIC]	alphv	Link
2023-08-22	[GROUPHC]	blackbasta	Link
2023-08-18	[Softverg Co., Ltd.]	noescape	Link
2023-08-13	[FYTISA Industrial Felts and FabricsSL]	noescape	Link
2023-08-13	[Infuance Communication Inc]	noescape	Link
2023-08-21	[Pierce College]	rhysida	Link
2023-08-21	[Department of Defence South African (DARPA)]	snatch	Link
2023-08-21	[apdparcel.com.au]	lockbit3	Link
2023-08-21	[TRIUNE TECHNOFAB PRIVATE LIMITED WAS HACKED]	alphv	Link
2023-08-21	[I&G Broker House]	ransomed	Link
2023-08-21	[A1 Data Provider]	ransomed	Link
2023-08-21	[Department of Defence South African]	snatch	Link
2023-08-21	[Davidoff Hutcher & Citron]	alphv	Link
2023-08-21	[Seiko Group Corporation]	alphv	Link
2023-08-20	[stockwellharris.com]	lockbit3	Link
2023-08-20	[hallbergengineering.com]	lockbit3	Link
2023-08-20	[cloudtopoffice.com]	lockbit3	Link
2023-08-20	[equip-reuse.com]	lockbit3	Link
2023-08-20	[cochraninc.com]	lockbit3	Link
2023-08-19	[Novi Pazar put ad]	medusa	Link
2023-08-19	[The International Civil Defense Organization]	medusa	Link
2023-08-19	[Sartrouville France]	medusa	Link
2023-08-19	[goldmedalbakery]	cuba	Link
2023-08-19	[s3groupltd.com]	lockbit3	Link
2023-08-19	[macuspana.gob.mx]	lockbit3	Link
2023-08-19	[phitoformulas.com.br]	lockbit3	Link
2023-08-18	[ABS Auto Auctions]	play	Link
2023-08-18	[DSA Law Pty Ltd]	play	Link
2023-08-18	[Miami Management]	play	Link
2023-08-18	[BTC Power]	play	Link
2023-08-18	[Stanford Transportation Inc]	play	Link
2023-08-18	[Bolton Group]	play	Link
2023-08-18	[Legends Limousine]	play	Link
2023-08-18	[Oneonline]	play	Link
2023-08-18	[purever.com]	lockbit3	Link
2023-08-18	[neolife.com]	lockbit3	Link
2023-08-09	[mitchcointernational.com]	lockbit3	Link
2023-08-15	[tedpella.com]	lockbit3	Link
2023-08-11	[au Domain Administration Ltd]	noescape	Link
2023-08-11	[Contact 121 Pty Ltd]	noescape	Link
2023-08-17	[umchealth.com]	lockbit3	Link
2023-08-17	[sgl.co.th]	lockbit3	Link
2023-08-17	[Agriloja.pt demo-leak]	everest	Link
2023-08-17	[RIMSS]	akira	Link
2023-08-17	[SFJAZZ.ORG]	lockbit3	Link
2023-08-17	[mybps.us]	lockbit3	Link
2023-08-17	[kriegerklatt.com]	lockbit3	Link
2023-08-17	[ALLIANCE]	blackbasta	Link
2023-08-17	[DEUTSCHELEASING]	blackbasta	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-17	[VDVEN]	blackbasta	Link
2023-08-17	[SYNQUESTLABS]	blackbasta	Link
2023-08-17	[TWINTOWER]	blackbasta	Link
2023-08-17	[Camino Nuevo CharterAcademy]	akira	Link
2023-08-17	[Smart-swgcr.org]	lockbit3	Link
2023-08-17	[The Clifton Public Schools]	akira	Link
2023-08-17	[MBO-PPS.COM]	clon	Link
2023-08-17	[MBOAMERICA.COM]	clon	Link
2023-08-17	[KOMORI.COM]	clon	Link
2023-08-16	[Dillon Supply]	metaencryptor	Link
2023-08-16	[Epicure]	metaencryptor	Link
2023-08-16	[Coswell]	metaencryptor	Link
2023-08-16	[BOB Automotive Group]	metaencryptor	Link
2023-08-16	[Seoul Semiconductor]	metaencryptor	Link
2023-08-16	[Kraiburg Austria GmbH]	metaencryptor	Link
2023-08-16	[Autohaus Ebert GmbH]	metaencryptor	Link
2023-08-16	[CVO Antwerpen]	metaencryptor	Link
2023-08-16	[ICON Creative Studio]	metaencryptor	Link
2023-08-16	[Heilmann Gruppe]	metaencryptor	Link
2023-08-16	[Schwälbchen Molkerei AG]	metaencryptor	Link
2023-08-16	[Münchner Verlagsgruppe GmbH]	metaencryptor	Link
2023-08-16	[Cequent]	akira	Link
2023-08-16	[Tally Energy Services]	akira	Link
2023-08-16	[CORDELLCORDELL]	alphv	Link
2023-08-16	[Municipality of Ferrara]	rhysida	Link
2023-08-16	[Hemmink]	incransom	Link
2023-08-16	[ToyotaLift Northeast]	8base	Link
2023-08-09	[FTRIA CO. LTD]	noescape	Link
2023-08-15	[Recaro]	alphv	Link
2023-08-15	[Postel SpA]	medusa	Link
2023-08-15	[ABA Research - Business Information 2]	alphv	Link
2023-08-15	[Keystone Insurance Services]	8base	Link
2023-08-15	[ANS]	8base	Link
2023-08-15	[Aspect Structural Engineers]	8base	Link
2023-08-08	[Fondation De Verdeil]	noescape	Link
2023-08-14	[Freeport-McMoran - NYSE: FCX]	alphv	Link
2023-08-14	[jhillburn.com]	lockbit3	Link
2023-08-14	[qbcqatar.com.qa]	lockbit3	Link
2023-08-07	[John L Lowery & Associates]	noescape	Link
2023-08-07	[Federal Bar Association]	noescape	Link
2023-08-14	[leecorpinc.com]	lockbit3	Link
2023-08-14	[econsult.com]	lockbit3	Link
2023-08-14	[Saint Xavier University]	alphv	Link
2023-08-14	[Agriloja.pt]	everest	Link
2023-08-14	[CB Energy Australlia]	medusa	Link
2023-08-14	[Borets (Levare.com)]	medusa	Link
2023-08-13	[majan.com]	lockbit3	Link
2023-08-13	[luterkort.se]	lockbit3	Link
2023-08-13	[difccourts.ae]	lockbit3	Link
2023-08-13	[zaun.co.uk]	lockbit3	Link
2023-08-13	[roxcel.com.tr]	lockbit3	Link
2023-08-13	[meaf.com]	lockbit3	Link
2023-08-13	[stmarysschool.co.za]	lockbit3	Link
2023-08-13	[rappenglitz.de]	lockbit3	Link
2023-08-13	[siampremier.co.th]	lockbit3	Link
2023-08-12	[National Institute of Social Services for Retirees and Pensioners]	rhysida	Link
2023-08-12	[Armortex]	bianlian	Link
2023-08-12	[arganoInterRel]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-11	[Rite Technology]	akira	Link
2023-08-11	[zain.com]	lockbit3	Link
2023-08-10	[Top Light]	play	Link
2023-08-10	[Algorry Zappia & Associates]	play	Link
2023-08-10	[EAI]	play	Link
2023-08-10	[The Belt Railway Company of Chicago]	akira	Link
2023-08-10	[Optimum Technology]	akira	Link
2023-08-10	[Boson]	akira	Link
2023-08-10	[Stockdale Podiatry]	8base	Link
2023-08-09	[oneatlas.com]	lockbit3	Link
2023-08-05	[Lower Yukon School District]	noescape	Link
2023-08-06	[Thermenhotel Stoiser]	incransom	Link
2023-08-09	[el-cerrito.org]	lockbit3	Link
2023-08-09	[fashions-uk.com]	lockbit3	Link
2023-08-09	[cbcstjohns.co.za]	lockbit3	Link
2023-08-09	[octoso.de]	lockbit3	Link
2023-08-09	[ricks-motorcycles.com]	lockbit3	Link
2023-08-09	[janus-engineering.com]	lockbit3	Link
2023-08-09	[csem.qc.ca]	lockbit3	Link
2023-08-09	[asfcustomers.com]	lockbit3	Link
2023-08-09	[sekuro.com.tr]	lockbit3	Link
2023-08-09	[TIMECO]	akira	Link
2023-08-09	[chula.ac.th]	lockbit3	Link
2023-08-09	[etisaleg.com]	lockbit3	Link
2023-08-09	[2plan.com]	lockbit3	Link
2023-08-08	[Sabalan Azmayesh]	arvinclub	Link
2023-08-09	[Optimum Health Solutions]	rhysida	Link
2023-08-09	[unitycouncil.org]	lockbit3	Link
2023-08-09	[independenceia.org]	lockbit3	Link
2023-08-09	[www.finitia.net]	abyss	Link
2023-08-09	[Ramtha]	rhysida	Link
2023-08-08	[Batesville didn't react on appeal and allows Full Leak]	ragnarlocker	Link
2023-08-08	[ZESA Holdings]	everest	Link
2023-08-08	[Magic Micro Computers]	alphv	Link
2023-08-08	[Emerson School District]	medusa	Link
2023-08-08	[CH informatica]	8base	Link
2023-08-07	[Thonburi Energy Storage Systems (TESM)]	qilin	Link
2023-08-07	[Räddningstjänsten Västra Blekinge]	akira	Link
2023-08-07	[Papel Prensa SA]	akira	Link
2023-08-01	[Kreacta]	noescape	Link
2023-08-07	[Parsian Bitumen]	arvinclub	Link
2023-08-07	[varian.com]	lockbit3	Link
2023-08-06	[Delaney Browne Recruitment]	8base	Link
2023-08-06	[IBL]	alphv	Link
2023-08-05	[Draje food industrial group]	arvinclub	Link
2023-08-06	[Oregon Sports Medicine]	8base	Link
2023-08-06	[premierbpo.com]	alphv	Link
2023-08-06	[SatCom Marketing]	8base	Link
2023-08-05	[Rayden Solicitors]	alphv	Link
2023-08-05	[haynesintl.com]	lockbit3	Link
2023-08-05	[Kovair Software Data Leak]	everest	Link
2023-08-05	[Henlaw]	alphv	Link
2023-08-04	[mipe.com]	lockbit3	Link
2023-08-04	[armortex.com]	lockbit3	Link
2023-08-04	[iqcontrols.com]	lockbit3	Link
2023-08-04	[scottevest.com]	lockbit3	Link
2023-08-04	[atser.com]	lockbit3	Link
2023-08-04	[Galicia en Goles]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-08-04	[tetco.com]	lockbit3	Link
2023-08-04	[SBS Construction]	alphv	Link
2023-08-04	[Koury Engineering]	akira	Link
2023-08-04	[Pharmatech Repblica Dominicana was hacked. All sensitive company and customer information]	alphv	Link
2023-08-04	[Grupo Garza Ponce was hacked! Due to a massive company vulnerability, more than 2 TB of se]	alphv	Link
2023-08-04	[seaside-kish co]	arvinclub	Link
2023-08-04	[Studio Domaine LLC]	nokoyawa	Link
2023-08-04	[THECHANGE]	alphv	Link
2023-08-04	[Ofimedic]	alphv	Link
2023-08-04	[Abatti Companies - Press Release]	monti	Link
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	Link
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	Link
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	Link
2023-08-03	[Venture General Agency]	akira	Link
2023-08-03	[Datawatch Systems]	akira	Link
2023-08-03	[admsc.com]	lockbit3	Link
2023-08-03	[United Tractors]	rhysida	Link
2023-08-03	[RevZero, Inc]	8base	Link
2023-08-03	[Rossman Realty Group, inc.]	8base	Link
2023-08-03	[riggsabney]	alphv	Link
2023-08-02	[fec-corp.com]	lockbit3	Link
2023-08-02	[bestmotel.de]	lockbit3	Link
2023-08-02	[Tempur Sealy International]	alphv	Link
2023-08-02	[constructioncrd.com]	lockbit3	Link
2023-08-02	[Helen F. Dalton Lawyers]	alphv	Link
2023-08-02	[TGRWA]	akira	Link
2023-08-02	[Guido]	akira	Link
2023-08-02	[Bickel & Brewer - Press Release]	monti	Link
2023-08-02	[SHERMAN.EDU]	clon	Link
2023-08-02	[COSI]	karakurt	Link
2023-08-02	[unicorpusa.com]	lockbit3	Link
2023-08-01	[Garage Living, The Dispenser USA]	play	Link
2023-08-01	[Aapd]	play	Link
2023-08-01	[Birch, Horton, Bittner & Cherot]	play	Link
2023-08-01	[DAL-TECH Engineering]	play	Link
2023-08-01	[Coral Resort]	play	Link
2023-08-01	[Professionnel France]	play	Link
2023-08-01	[ACTIVA Group]	play	Link
2023-08-01	[Aquatlantis]	play	Link
2023-08-01	[Kogetsu]	mallox	Link
2023-08-01	[Parathon by JDA eHealth Systems]	akira	Link
2023-08-01	[KIMCO Staffing Service]	alphv	Link
2023-08-01	[Pea River Electric Cooperative]	nokoyawa	Link
2023-08-01	[MBS Equipment TTI]	8base	Link
2023-08-01	[gerb.bg]	lockbit3	Link
2023-08-01	[persingerlaw.com]	lockbit3	Link
2023-08-01	[Jacklett Construction LLC]	8base	Link

Quellen

Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - packetstormsecurity.com
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

Impressum



Herausgeber:

Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail

info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.