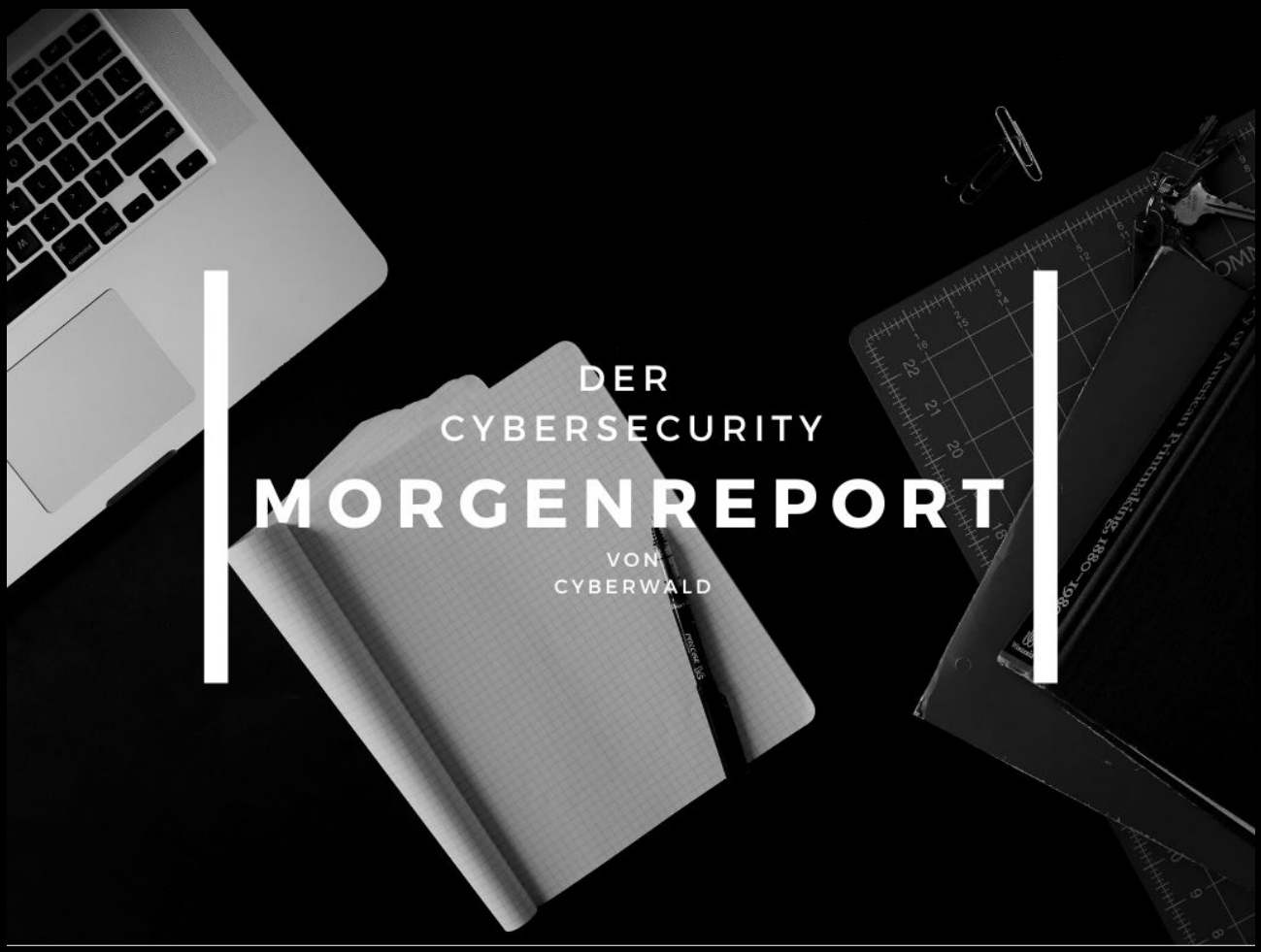
Cybersecurity Morgenreport



Ausgabe: 20231014

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

Sicherheitsupdate für WordPress erschienen und angreifbares Plug-in repariert
In der aktuellen WordPress-Version 6.3.2 haben die Entwickler mehrere Sicherheitslücken geschlossen.
- Link

—

40 Schwachstellen in IBM-Sicherheitslösung QRadar SIEM geschlossen
Mehrere Komponenten in IBM QRadar SIEM weisen Sicherheitslücken auf und gefährden das Security-Information-and-Event-Management-System.
- Link

—

Sicherheitsupdates: Backdoor-Lücke bedroht Netzwerkgeräte von Juniper
Schwachstellen im Netzwerkbetriebssystem Junos OS bedrohen Routing-, Switching- und Sicherheitsgeräte von Juniper.
- Link

—

Patchday F5: Sicherheitslücken in BIG-IP ermöglichen Angreifern Codeausführung
F5 hat mehrere Sicherheitsmeldungen zu Lecks in BIG-IP-Appliances und -Software veröffentlicht. Aktualisierungen stehen bereit.
- Link

—

Sicherheitsupdates Fortinet: Angreifer können Passwörter im Klartext einsehen
Fortinet hat wichtige Sicherheitspatches für FortiOS und FortiProxy veröffentlicht.
- Link

—

Rapid Reset: Angreifer nutzen Lücke im HTTP/2-Protokoll seit August 2023 aus
Eine DDoS-Sicherheitslücke mit Rekordvolumen im HTTP/2-Protokoll gefährdet unzählige Server. Erste Sicherheitspatches sind verfügbar.
- Link

—

Citrix dichtet kritisches Leck in Netscaler ab
In Netscaler ADC und Gateway klaffen Sicherheitslücken, ebenso im Hypervisor von Citrix. Aktualisierte Software-Pakete schließen sie.
- Link

—

Patchday Adobe: Schadcode-Attacken auf Magento-Shops und Photoshop möglich
Die Entwickler von Adobe haben in Bridge, Commerce, Magento Open Source und Photoshop mehrere Sicherheitslücken geschlossen.
- Link

—

Webbrowser: Google-Chrome-Update schließt kritische Sicherheitslücke
Google hat das wöchentliche Chrome-Update herausgegeben. Es schließt 20 Sicherheitslücken, von denen mindestens eine als kritisch gilt.
- Link

—

Patchday Microsoft: Attacken auf Skype for Business und WordPad
Microsoft hat wichtige Sicherheitsupdates für etwa Azure, Office und Windows veröffentlicht.
- 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-2023-42793	0.972090000	0.997580000	Link
CVE-2023-38035	0.970820000	0.996880000	Link
CVE-2023-35078	0.959430000	0.992660000	Link
CVE-2023-34362	0.921790000	0.986270000	Link
CVE-2023-33246	0.971460000	0.997210000	Link
CVE-2023-32315	0.960720000	0.993000000	Link
CVE-2023-30625	0.932650000	0.987730000	Link
CVE-2023-30013	0.936180000	0.988200000	Link
CVE-2023-28771	0.926550000	0.986870000	Link
CVE-2023-27524	0.932860000	0.987790000	Link
CVE-2023-27372	0.971800000	0.997440000	Link
CVE-2023-27350	0.971270000	0.997120000	Link
CVE-2023-26469	0.918080000	0.985860000	Link
CVE-2023-26360	0.919780000	0.986060000	Link
CVE-2023-25717	0.961680000	0.993230000	Link
CVE-2023-25194	0.924830000	0.986620000	Link
CVE-2023-2479	0.961630000	0.993200000	Link
CVE-2023-24489	0.968600000	0.995850000	Link
CVE-2023-22515	0.935270000	0.988090000	Link
CVE-2023-21839	0.951010000	0.990690000	Link
CVE-2023-21823	0.929300000	0.987270000	Link
CVE-2023-21554	0.961360000	0.993160000	Link
CVE-2023-20887	0.932820000	0.987780000	Link
CVE-2023-0669	0.968230000	0.995640000	Link

BSI - Warn- und Informationsdienst (WID)

Fri, 13 Oct 2023
[UPDATE] [hoch] Mozilla Firefox: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen.
- Link

Fri, 13 Oct 2023
[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] OpenSSH: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSH ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen oder seine Privilegien zu erweitern.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] Red Hat Enterprise Linux (libvpx): Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Komponente libvpx ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] Xen: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Xen ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Fri, 13 Oct 2023
[UPDATE] [hoch] Juniper Patchday Oktober 2023
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Juniper Produkten ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und seine Privilegien zu erweitern.
- Link

—

Fri, 13 Oct 2023

[NEU] [hoch] Hitachi Energy AFS: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Hitachi Energy AFS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.
- Link
—
Thu, 12 Oct 2023
[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel und Oracle Linux ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsvorkehrungen zu umgehen.
- Link
—
Thu, 12 Oct 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.
- Link
—
Thu, 12 Oct 2023
[UPDATE] [hoch] Python: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.
- Link
—
Thu, 12 Oct 2023
[UPDATE] [hoch] Ghostscript: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ghostscript ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 12 Oct 2023
[NEU] [hoch] Zabbix: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.
- Link
—
Thu, 12 Oct 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 12 Oct 2023
[NEU] [hoch] Google Android Pixel: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android Pixel ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.
- Link
—
Thu, 12 Oct 2023
[NEU] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/13/2023	[SUSE SLED12 / SLES12 Security Update : python-reportlab (SUSE-SU-2023:4048-1)]	critical
10/13/2023	[Debian DSA-5527-1 : webkit2gtk - security update]	critical
10/13/2023	[NetScaler ADC and NetScaler Gateway Multiple Vulnerabilities (CTX579459)]	critical
10/13/2023	[Oracle Linux 7 : firefox (ELSA-2023-5477)]	critical
10/13/2023	[Cisco Emergency Responder Static Credentials (cisco-sa-cer-priv-esc-B9t3hqk9)]	critical
10/13/2023	[F5 Networks BIG-IP : BIG-IP Configuration utility RCE (K000135689)]	critical
10/13/2023	[Oracle Linux 6 : busybox (ELSA-2023-5178)]	critical
10/13/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xen (SUSE-SU-2023:4054-1)]	high
10/13/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xen (SUSE-SU-2023:4055-1)]	high
10/13/2023	[Debian DSA-5526-1 : chromium - security update]	high
10/13/2023	[Security Updates for Microsoft Visual Studio Products (October 2023)]	high
10/13/2023	[Samba 4.x < 4.17.12 / 4.18.x < 4.18.8 / 4.19.x < 4.19.1 Multiple Vulnerabilities]	high
10/13/2023	[Samba < 4.17.12 / 4.18.x < 4.18.8 / 4.19.x < 4.19.1 Incorrect Permissions Handling]	high
10/13/2023	[Security Update for Microsoft .NET 7 Core (October 2023)]	high
10/13/2023	[Security Update for Microsoft .NET 6 Core (October 2023)]	high
10/13/2023	[Trellix Endpoint Security for Windows < 10.7.0 September 2023 Update Code Injection (SB10405)]	high
10/13/2023	[Golang 1.20.x < 1.20.9, 1.21.x < 1.21.2 RCE]	high
10/13/2023	[Security Updates for Microsoft Office Products C2R Multiple Vulnerabilities (October 2023)]	high
10/13/2023	[Oracle Linux 7 / 8 : Unbreakable Enterprise kernel (ELSA-2023-12874)]	high
10/13/2023	[Security Updates for Microsoft SQL Server ODBC Driver (October 2023)]	high
10/13/2023	[F5 Networks BIG-IP : BIG-IP iControl REST Privilege Escalation (K26910459)]	high
10/13/2023	[F5 Networks BIG-IP IPsec DoS (K000132420)]	high
10/13/2023	[F5 Networks BIG-IP Edge Client for macOS Privilege Escalation (K000135040)]	high
10/13/2023	[F5 Networks BIG-IP HTTP/2 DoS (K000133467)]	high
10/13/2023	[F5 Networks BIG-IP TCP profile vulnerability (K000134652)]	high
10/13/2023	[F5 Networks BIG-IP : BIG-IP Edge Client for macOS Privilege Escalation (K000136185)]	high
10/13/2023	[F5 Networks BIG-IP : BIG-IP Appliance Mode External Monitor Vulnerability (K41072952)]	high
10/13/2023	[F5 Networks BIG-IP : BIG-IP HTTP/2 DoS (K000137106)]	high
10/13/2023	[AlmaLinux 9 : galera and mariadb (ALSA-2023:5684)]	high
10/13/2023	[AlmaLinux 8 : mariadb:10.5 (ALSA-2023:5683)]	high
10/13/2023	[Microsoft Edge (Chromium) < 118.0.2088.46 Multiple Vulnerabilities]	high
10/13/2023	[AlmaLinux 9 : bind (ALSA-2023:5689)]	high
10/13/2023	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2023-12875)]	high
10/13/2023	[CBL Mariner 2.0 Security Update: hyperv-daemons (CVE-2023-42753)]	high
10/13/2023	[CBL Mariner 2.0 Security Update: glibc (CVE-2023-4911)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Fri, 13 Oct 2023
PyTorch Model Server Registration / Deserialization Remote Code Execution
The PyTorch model server contains multiple vulnerabilities that can be chained together to permit an unauthenticated remote attacker arbitrary Java code execution. The first vulnerability is that the management interface is bound to all IP addresses and not just the loop back interface as the documentation suggests. The second vulnerability (CVE-2023-43654) allows attackers with access to the management interface to register MAR model files from arbitrary servers. The third vulnerability is that when an MAR file is loaded, it can contain a YAML configuration file that when deserialized by snakeyaml, can lead to loading an arbitrary Java class.
- Link
—
” “Fri, 13 Oct 2023
Apache Superset 2.0.0 Remote Code Execution
Apache Superset versions 2.0.0 and below utilize Flask with a known default secret key which is used to sign HTTP cookies. These cookies can therefore be forged. If a user is able to login to the site, they can decode the cookie, set their user_id to that of an administrator, and re-sign the cookie. This valid cookie can then be used to login as the targeted user. From there the Superset database is mounted, and credentials are pulled. A dashboard is then created. Lastly a pickled python payload can be set for that dashboard within Superset’s database which will trigger the remote code execution. An attempt to clean up ALL of the dashboard key values and reset them to their previous values happens during the cleanup phase.
- Link
—
” “Fri, 13 Oct 2023
WordPress Core 6.3.1 XSS / DoS / Arbitrary Shortcode Execution
WordPress Core versions prior to 6.3.2 suffer from arbitrary shortcode execution, cross site scripting, denial of service, and information leakage vulnerabilities. Versions prior to 6.3.2 are vulnerable.
- Link
—
” “Thu, 12 Oct 2023
Dawa Pharma 1.0-2022 SQL Injection
Dawa Pharma version 1.0-2022 suffers from a remote SQL injection vulnerability.
- Link
—
” “Thu, 12 Oct 2023
Lost And Found Information System 1.0 Insecure Direct Object Reference
Lost and Found Information System version 1.0 suffers from an insecure direct object reference vulnerability that allows for account takeover.
- Link
—
” “Thu, 12 Oct 2023
Clinic’s Patient Management System 1.0 Shell Upload
Clinic’s Patient Management System version 1.0 suffers from a remote shell upload vulnerability.
- Link
—
” “Wed, 11 Oct 2023
Smart School 6.4.1 SQL Injection
Smart School version 6.4.1 suffers from multiple remote SQL injection vulnerabilities.
- Link
—
” “Wed, 11 Oct 2023
Gaatitrack 1.0-2023 SQL Injection
Gaatitrack version 1.0-2023 suffers from a remote SQL injection vulnerability.
- Link
—
” “Tue, 10 Oct 2023
Cacti 1.2.24 Command Injection
Cacti version 1.2.24 authenticated command injection exploit that uses SNMP options.

- Link

—

” “Tue, 10 Oct 2023

BoidCMS 2.0.0 Shell Upload

BoidCMS versions 2.0.0 and below suffer from a remote shell upload vulnerability.

- Link

—

” “Tue, 10 Oct 2023

Webedition CMS 2.9.8.8 Server-Side Request Forgery

Webedition CMS version 2.9.8.8 suffers from a blind server-side request forgery vulnerability.

- Link

—

” “Tue, 10 Oct 2023

OpenPLC WebServer 3 Denial Of Service

OpenPLC WebServer version 3 suffers from a denial of service vulnerability.

- Link

—

” “Tue, 10 Oct 2023

Atcom 2.7.x.x Command Injection

Atcom version 2.7.x.x suffers from an authenticated remote code injection vulnerability.

- Link

—

” “Tue, 10 Oct 2023

WordPress Sonaar Music 4.7 Cross Site Scripting

WordPress Sonaar Music plugin version 4.7 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 10 Oct 2023

Coppermine Gallery 1.6.25 Remote Code Execution

Coppermine Gallery version 1.6.25 remote code execution exploit.

- Link

—

” “Tue, 10 Oct 2023

Minio 2022-07-29T19-40-48Z Path Traversal

Minio version 2022-07-29T19-40-48Z suffers from a path traversal vulnerability.

- Link

—

” “Tue, 10 Oct 2023

WordPress Masterstudy LMS 3.0.17 Account Creation

WordPress Masterstudy LMS plugin version 3.0.17 suffers from an unauthenticated instructor account creation vulnerability.

- Link

—

” “Tue, 10 Oct 2023

Microsoft Windows 11 apds.dll DLL Hijacking

Microsoft Windows 11 apds.dll DLL hijacking exploit.

- Link

—

” “Tue, 10 Oct 2023

GLPI GZIP(Py3) 9.4.5 Remote Code Execution

GLPI GZIP(Py3) version 9.4.5 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 09 Oct 2023

Kibana Prototype Pollution / Remote Code Execution

Kibana versions prior to 7.6.3 suffer from a prototype pollution bug within the Upgrade Assistant. By setting a new constructor.prototype.sourceURL value you can execute arbitrary code. Code execution is possible through two different ways. Either by sending data directly to Elastic, or using Kibana to submit the same queries. Either method enters the polluted prototype for Kibana to read. Kibana will either need to be restarted, or collection happens (unknown time) for the payload to execute. Once it does, cleanup must delete the .kibana_1 index for Kibana to restart successfully. Once a callback does occur, cleanup will happen allowing Kibana to

be successfully restarted on next attempt.
- Link
—
” “Mon, 09 Oct 2023
eClass Junior 4.0 SQL Injection
eClass Junior version 4.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 09 Oct 2023
eClass IP 2.5 SQL Injection
eClass IP version 2.5 suffers from a remote SQL injection vulnerability.
- Link
—
” “Mon, 09 Oct 2023
Chicv Management System Login 4.5.6 Insecure Direct Object Reference
Chicv Management System Login version 4.5.6 suffers from an insecure direct object reference vulnerability.
- Link
—
” “Mon, 09 Oct 2023
Aicte India LMS 3.0 Cross Site Scripting
Aicte India LMS version 3.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Fri, 06 Oct 2023
glibc ld.so Local Privilege Escalation
Dubbed Looney Tunables, Qualys discovered a buffer overflow vulnerability in the glibc dynamic loader’s processing of the GLIBC_TUNABLES environment variable. This vulnerability was introduced in April 2021 (glibc 2.34) by commit 2ed18c.
- Link
—
”

0-Day

“Wed, 11 Oct 2023
ZDI-23-1558: Siemens Tecnomatix Plant Simulation PAR File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1557: Siemens Tecnomatix Plant Simulation PRT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1556: Siemens Tecnomatix Plant Simulation PAR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1555: Microsoft Windows DirectX GpuMmu Race Condition Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1554: Microsoft Windows bStretch Improper Input Validation Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1553: Microsoft Windows DEVLOCKBLTOBJ Race Condition Local Privilege Escala-

tion Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1552: Microsoft Windows UMPDDrvPlgBlt Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1551: Microsoft Windows UMPDDrvStretchBlt Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1550: Microsoft Windows UMPDDrvBitBlt Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1549: Microsoft Windows UMPDDrvStretchBltROP Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1548: Microsoft Windows UMPDDrvCopyBits Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1547: Microsoft Windows UMPDDrvStretchBlt Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1546: Microsoft Windows UMPDDrvStretchBltROP Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1545: Microsoft Windows IsSurfaceLockable Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1544: Microsoft Windows UMPDDrvPlgBlt Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1543: Microsoft Windows UMPDDrvBitBlt Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1542: Microsoft Windows UMPDDrvCopyBits Type Confusion Local Privilege Escalation Vulnerability
- Link
—
” “Wed, 11 Oct 2023
ZDI-23-1541: (Pwn2Own) Microsoft Teams Incorrect Privilege Assignment Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 11 Oct 2023

ZDI-23-1540: (Pwn2Own) Microsoft Teams Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Oct 2023

ZDI-23-1539: Adobe Photoshop PSD File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Oct 2023

ZDI-23-1538: Adobe Bridge Font Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 11 Oct 2023

ZDI-23-1537: Adobe Bridge Font Parsing Use-After-Free Information Disclosure Vulnerability

- Link

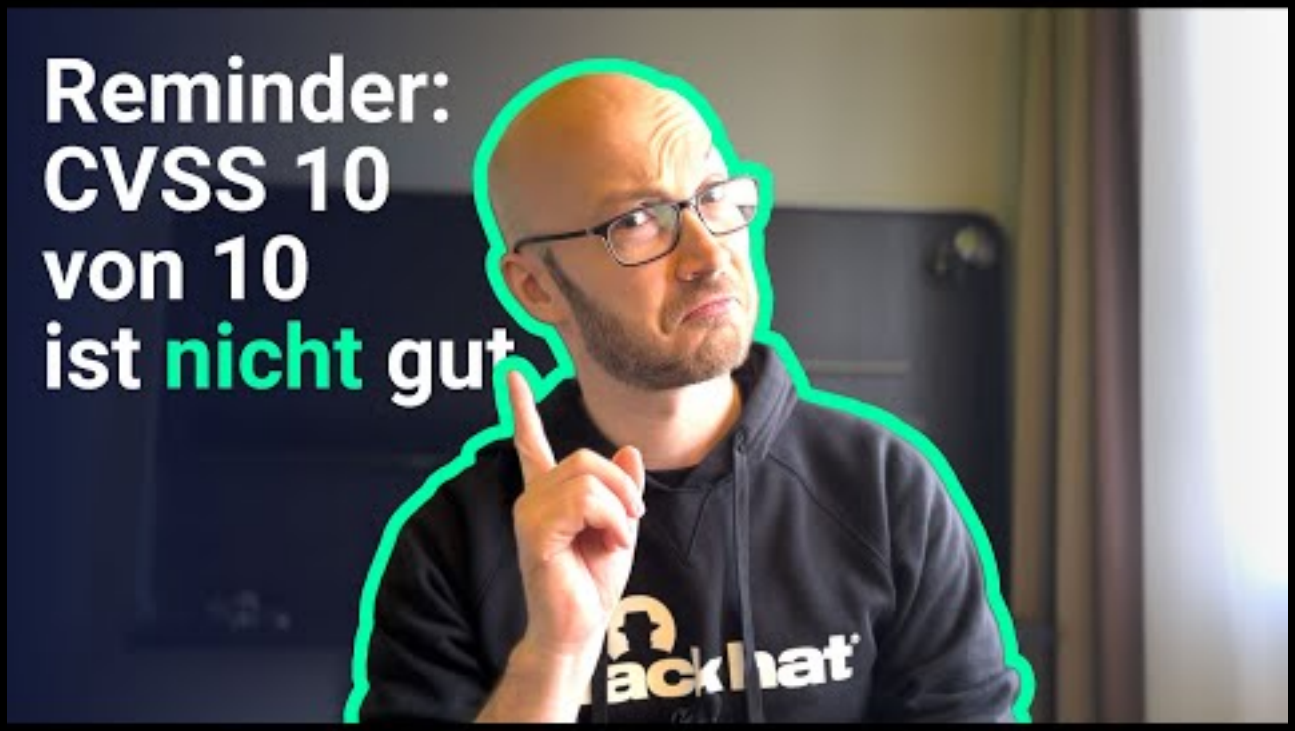
—

”

Die Hacks der Woche

mit Martin Haunschmid

In der IT-Security ist 10 von 10 NICHT IMMER etwas Gutes



Zum Youtube Video

Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2023-10-12	Service Départemental d'Incendie et de Secours des Pyrénées-Atlantiques (SDIS64)	[FRA]	Link
2023-10-10	Simpson Manufacturing Co.	[USA]	Link
2023-10-09	De La Salle University (DLSU)	[PHL]	Link
2023-10-08	Volex PLC	[GBR]	Link
2023-10-07	Centre hospitalier de l'Ouest Vosgien	[FRA]	Link
2023-10-06	Clinique universitaire de Francfort	[DEU]	Link
2023-10-05	Dansk Scanning	[DNK]	Link
2023-10-03	Metro Transit	[USA]	Link
2023-10-02	Estes Express Lines	[USA]	Link
2023-10-02	Hochschule de Karlsruhe	[DEU]	Link
2023-10-02	Provincia di Cosenza	[ITA]	Link
2023-10-02	Degenia	[DEU]	Link
2023-10-02	Le Premier Circuit Judiciaire de Floride	[USA]	Link
2023-10-01	Lyca Mobile UK	[GBR]	Link

Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-10-14	[Intech]	snatch	Link
2023-10-13	[Catholic Charities]	incransom	Link
2023-10-13	[Kimia Tadbir Kiyan]	arvinclub	Link
2023-10-05	[Korea Petroleum Industrial Co. Ltd]	noescape	Link
2023-10-13	[Cleveland City Schools]	incransom	Link
2023-10-13	[Alconex Specialty Products]	trigona	Link
2023-10-13	[Multidev Technologies]	blacksuit	Link
2023-10-13	[Morrison Community Hospital]	alphv	Link
2023-10-13	[Hospital Italiano de Buenos Aires]	knight	Link
2023-10-13	[AKBASOGLU HOLDING Trans KA]	knight	Link
2023-10-13	[Metroclub.org]	ransomed	Link
2023-10-13	[Optimity UK]	ransomed	Link
2023-10-13	[Baumit Bulgaria]	ransomed	Link
2023-10-13	[novoingresso.com.br]	ransomed	Link
2023-10-13	[webpag.com.br]	ransomed	Link
2023-10-13	[rodoviariaonline.com.br]	ransomed	Link
2023-10-13	[Kasida.bg Database Leaked, Download]	ransomed	Link
2023-10-13	[I&G Brokers Database, Download Now]	ransomed	Link
2023-10-13	[pilini.bg Database, Download Now!]	ransomed	Link
2023-10-13	[iLife.bg]	ransomed	Link
2023-10-13	[Fuck Palestine! We buy your access!!]	ransomed	Link
2023-10-13	[NEW TWITTER]	ransomed	Link
2023-10-12	[Vicon industries inc.]	incransom	Link
2023-10-05	[Seattle Housing Authority]	noescape	Link
2023-10-12	[FPZ]	trigona	Link
2023-10-12	[Tri-Way Manufacturing Technologies]	moneymessage	Link
2023-10-12	[Neodata]	medusa	Link
2023-10-12	[Evasión]	medusa	Link
2023-10-12	[SIMTA]	medusa	Link
2023-10-12	[ZOUARY & Associés]	medusa	Link
2023-10-10	[Comtek Advanced Structures, a Latecoere Company]	8base	Link
2023-10-10	[KTUA Landscape Architecture and Planning]	8base	Link
2023-10-11	[Scotbeef Ltd. - Leaks]	ragnarlocker	Link
2023-10-09	[LDLC ASVEL]	noescape	Link
2023-10-11	[Institut Technologique FCBA]	alphv	Link
2023-10-09	[Instant Access Co]	noescape	Link
2023-10-11	[Eicon Controle Inteligentes]	ragnarlocker	Link
2023-10-11	[Air Canada]	bianlian	Link
2023-10-11	[Pelindo]	bianlian	Link
2023-10-11	[Instron & ITW Inc]	bianlian	Link
2023-10-11	[Mid-America Real Estate Group]	alphv	Link
2023-10-11	[Village Building Co.]	incransom	Link
2023-10-11	[STANTONWILLIAMS]	blackbasta	Link
2023-10-11	[REH]	blackbasta	Link
2023-10-11	[HAEFFNER-ASP]	blackbasta	Link
2023-10-11	[GREGAGG]	blackbasta	Link
2023-10-11	[Catarineau & Givens P.A]	alphv	Link
2023-10-11	[Sobieski]	incransom	Link
2023-10-11	[We monetize your corporate access]	everest	Link
2023-10-09	[Metro Transit]	play	Link
2023-10-01	[Effigest Capital Services]	noescape	Link
2023-10-10	[Alliance Virgil Roberts Leadership Academy]	snatch	Link
2023-10-10	[foremostgroups.com]	lockbit3	Link
2023-10-10	[National Health Mission. Department of Health & Family Welfare, Govt. of U.P]	knight	Link
2023-10-10	[mountstmarys]	cuba	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-10-10	[ExdionInsurance]	8base	Link
2023-10-10	[National Health Mission. Department of Heath & Family Welfare, Govt. of U.P]	knight	Link
2023-10-01	[Elbe-Obst Fruchtverarbeitung GmbH]	noescape	Link
2023-10-03	[Ordine Degli Psicologi Della Lombardia]	noescape	Link
2023-10-09	[Saltire Energy]	play	Link
2023-10-09	[Starr Finley]	play	Link
2023-10-09	[WCM Europe]	play	Link
2023-10-09	[NachtExpress Austria GmbH]	play	Link
2023-10-09	[Centek industries]	play	Link
2023-10-09	[M??? T??????]	play	Link
2023-10-10	[Hughes Gill Cochrane Tinetti]	play	Link
2023-10-01	[Penfield Fire Co]	noescape	Link
2023-10-01	[Centre Du Sablon]	noescape	Link
2023-10-06	[GEACAM]	noescape	Link
2023-10-09	[Guhring was hacked. Thousands of confidential files stolen.]	knight	Link
2023-10-09	[Wyndemere Senior Care, LLC]	alphv	Link
2023-10-09	[First Judicial Circuit - Florida Court]	alphv	Link
2023-10-09	[atlantatech.edu]	lockbit3	Link
2023-10-09	[starplast.ft]	lockbit3	Link
2023-10-09	[WT PARTNERSHIP]	qilin	Link
2023-10-09	[Superline - Press Release]	monti	Link
2023-10-09	[dothanhauto.com]	lockbit3	Link
2023-10-09	[vsmpo-tirus.com]	lockbit3	Link
2023-10-09	[Law Society of South Africa]	alphv	Link
2023-10-09	[enerjet.com.pe]	lockbit3	Link
2023-10-09	[i-Can Advisory Group inc]	alphv	Link
2023-10-09	[BrData Tecnologia]	alphv	Link
2023-10-09	[Southern Arkansas University]	rhysida	Link
2023-10-08	[securicon.co.za]	lockbit3	Link
2023-10-08	[Islamic Azad University of Shiraz]	arvinclub	Link
2023-10-08	[urc-automation.com]	lockbit3	Link
2023-10-08	[IKM]	alphv	Link
2023-10-08	[Petersen Johnson]	8base	Link
2023-10-07	[University Obrany - Part 2 (Tiny Leak)]	monti	Link
2023-10-07	[DallBogg Breach]	ransomed	Link
2023-10-07	[Partnership With Breachforums]	ransomed	Link
2023-10-07	[The Hurley Group]	cactus	Link
2023-10-07	[Healix]	akira	Link
2023-10-06	[International Presence Ltd - Leaked]	ragnarlocker	Link
2023-10-06	[For UNOB]	monti	Link
2023-10-04	[NTT Docomo]	ransomed	Link
2023-10-05	[(SALE) District Of Columbia Elections 600k lines VOTERS DATA]	ransomed	Link
2023-10-06	[Agència Catalana de Notícies (ACN)]	medusa	Link
2023-10-06	[cote-expert-equipements.com]	lockbit3	Link
2023-10-06	[sinedieadvisor.com]	lockbit3	Link
2023-10-06	[tatatelebusiness.com]	lockbit3	Link
2023-10-06	[eemotors.com]	lockbit3	Link
2023-10-06	[bm.co.th]	lockbit3	Link
2023-10-06	[picosoft.biz]	lockbit3	Link
2023-10-06	[litung.com.tw]	lockbit3	Link
2023-10-05	[Granger Medical Clinic]	noescape	Link
2023-10-06	[Camara Municipal de Gondomar]	rhysida	Link
2023-10-05	[sirva.com]	lockbit3	Link
2023-10-05	[Low Keng Huat (Singapore) Limited]	bianlian	Link
2023-10-05	[Cornerstone Projects Group]	cactus	Link
2023-10-05	[RICOR Global Limited]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-10-05	[Learning Partnership West - Leaked]	ragnarlocker	Link
2023-10-05	[Terwilliger Land Survey Engineers]	akira	Link
2023-10-04	[DiTRONICS Financial Services]	qilin	Link
2023-10-04	[suncoast-chc.org]	lockbit3	Link
2023-10-04	[Meridian Cooperative]	blackbyte	Link
2023-10-04	[Roof Management]	play	Link
2023-10-04	[Security Instrument]	play	Link
2023-10-04	[Filtration Control]	play	Link
2023-10-04	[Cinepolis USA]	play	Link
2023-10-04	[CHARMANT Group]	play	Link
2023-10-04	[Stavanger Municipality]	play	Link
2023-10-04	[Gruskin Group]	akira	Link
2023-10-04	[McLaren Health Care Corporation]	alphv	Link
2023-10-04	[US Liner Company & American Made LLC]	0mega	Link
2023-10-04	[General Directorate of Migration of the Dominican Republic]	rhysida	Link
2023-10-03	[University of Defence - Part 1]	monti	Link
2023-10-03	[Toscana Promozione]	moneymessage	Link
2023-10-03	[MD LOGISTICS]	moneymessage	Link
2023-10-03	[Maxco Supply]	moneymessage	Link
2023-10-03	[Groupe Fructa Partner - Leaked]	ragnarlocker	Link
2023-10-03	[Somagic]	medusa	Link
2023-10-03	[The One Group]	alphv	Link
2023-10-03	[aicsacorp.com]	lockbit3	Link
2023-10-03	[co.rock.wi.us]	cuba	Link
2023-10-03	[Sabian Inc]	8base	Link
2023-10-03	[Ted Pella Inc.]	8base	Link
2023-10-03	[GDL Logística Integrada S.A]	knight	Link
2023-10-03	[Measuresoft]	mallox	Link
2023-10-02	[RAT.]	donutleaks	Link
2023-10-02	[AllCare Pharmacy]	lorenz	Link
2023-10-02	[Confidential files]	medusalocker	Link
2023-10-02	[Pain Care]	alphv	Link
2023-10-02	[Windak]	medusa	Link
2023-10-02	[Pasouk biological company]	arvinclub	Link
2023-10-02	[Karam Chand Thapar & Bros Coal Sales]	medusa	Link
2023-10-02	[Kirkholm Maskiningeniører]	mallox	Link
2023-10-02	[Federal University of Mato Grosso do Sul]	rhysida	Link
2023-10-01	[erga.com]	lockbit3	Link
2023-10-01	[thermae.nl]	lockbit3	Link
2023-10-01	[ckgroup.com.tw]	lockbit3	Link
2023-10-01	[raeburns.co.uk]	lockbit3	Link
2023-10-01	[tayloredservices.com]	lockbit3	Link
2023-10-01	[fcps1.org]	lockbit3	Link
2023-10-01	[laspesainfamiglia.coop]	lockbit3	Link
2023-10-01	[Cascade Family Dental - Press Release]	monti	Link
2023-10-01	[Rainbow Travel Service - Press Release]	monti	Link
2023-10-01	[Shirin Travel Agency]	arvinclub	Link
2023-10-01	[Flamingo Holland]	trigona	Link
2023-10-01	[Aria Care Partners]	trigona	Link
2023-10-01	[Portesa]	trigona	Link
2023-10-01	[Grupo Boreal]	trigona	Link
2023-10-01	[Quest International]	trigona	Link
2023-10-01	[Arga Medicali]	alphv	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.