



Ausgabe: 20231024

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

VMware dichtet hochriskante Lecks in Aria, Fusion und Workstation ab

VMware hat Updates für VMWare Aria Operations for Logs, VMware Fusion sowie VMware Workstation veröffentlicht. Sie schließen teils hochriskante Lücken.

- [Link](#)

Neue Version von SolarWinds Access Rights Manager behebt Codeschmuggel-Lücken

Die Software zur Verwaltung von Zugriffsberechtigungen hat unter anderem Fehler, die eine Rechteausweitung ermöglichten. Admins sollten zügig handeln.

- [Link](#)

Sophos Firewall: PDF-Passwortschutz der SPX-Funktion umgehbar

Sophos verteilt aktualisierte Firmware für die Firewalls. Im Secure PDF eXchange können Angreifer den Schutz umgehen und unbefugt PDF-Dateien entschlüsseln.

- [Link](#)

AMD-Grafiktreiber: Codeschmuggel durch Sicherheitslücke möglich

AMD warnt vor einer Sicherheitslücke in den eigenen Grafiktreibern. Angreifer könnten Code einschleusen und mit erhöhten Rechten ausführen.

- [Link](#)

Patchday: 387 Sicherheitsflicken von Oracle

Der vierteljährliche Patchday von Oracle hat stattgefunden. Er bringt im Oktober 387 Updates für mehr als 120 Produkte.

- [Link](#)

Sonicwall: SonicOS-Lücken ermöglichen DoS-Angriffe

Sonicwall hat Updates für SonicOS veröffentlicht, die Sicherheitslücken schließen. Die Lecks erlauben Angreifern, verwundbare Geräte lahmzulegen.

- [Link](#)

Cisco: Schwere Sicherheitslücke in IOS XE ermöglicht Netzwerk-Übernahme

Geräte mit IOS XE und Web-UI können von Angreifern ohne Weiteres aus der Ferne übernommen werden. Cisco hat keine Patches, aber Empfehlungen für Betroffene.

- [Link](#)

Wordpress: Übernahme durch Lücke in Royal Elementor Addons and Template

Im Wordpress-Plug-in Royal Elementor Addons and Template missbrauchen Cyberkriminelle eine kritische Lücke. Sie nutzen sie zur Übernahme von Instanzen.

- [Link](#)

Samba: Neue Versionen beheben mehrere Sicherheitslücken

Durch verschiedene Programmierfehler konnten Angreifer auf geheime Informationen bis hin zum Kerberos-TGT-Passwort zugreifen. Aktualisierungen stehen bereit.

- [Link](#)

Sicherheitsupdate für WordPress erschienen und angreifbares Plug-in repariert

In der aktuellen WordPress-Version 6.3.2 haben die Entwickler mehrere Sicherheitslücken geschlossen.

- [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	0.972490000	0.997810000	Link
CVE-2023-38035	0.970820000	0.996880000	Link
CVE-2023-35078	0.959430000	0.992690000	Link
CVE-2023-34362	0.921790000	0.986360000	Link
CVE-2023-33246	0.971460000	0.997230000	Link
CVE-2023-32315	0.960720000	0.993040000	Link
CVE-2023-30625	0.932650000	0.987810000	Link
CVE-2023-30013	0.936180000	0.988260000	Link
CVE-2023-28771	0.926550000	0.986980000	Link
CVE-2023-27524	0.912940000	0.985480000	Link
CVE-2023-27372	0.970840000	0.996880000	Link
CVE-2023-27350	0.971270000	0.997120000	Link
CVE-2023-26469	0.918080000	0.985940000	Link
CVE-2023-26360	0.919780000	0.986150000	Link
CVE-2023-25717	0.961680000	0.993280000	Link
CVE-2023-25194	0.916870000	0.985800000	Link
CVE-2023-2479	0.961630000	0.993250000	Link
CVE-2023-24489	0.970040000	0.996480000	Link
CVE-2023-22515	0.955290000	0.991740000	Link
CVE-2023-21839	0.952950000	0.991150000	Link
CVE-2023-21823	0.950040000	0.990550000	Link
CVE-2023-21554	0.961360000	0.993200000	Link
CVE-2023-20887	0.932820000	0.987860000	Link
CVE-2023-0669	0.965820000	0.994760000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 23 Oct 2023

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonym 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](#)

Mon, 23 Oct 2023

[NEU] [hoch] Red Hat Satellite: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Mon, 23 Oct 2023

[NEU] [hoch] Squid: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

Mon, 23 Oct 2023

[UPDATE] [kritisch] Cisco IOS XE: Schwachstellen ermöglichen Administrativen Zugriff

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Cisco IOS XE ausnutzen, um Administrativen Zugriff zu erlangen.

- [Link](#)

Mon, 23 Oct 2023

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Mon, 23 Oct 2023

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um einen Denial of Service Angriff durchzuführen, einen Cross-Site-Scripting-Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 23 Oct 2023

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 23 Oct 2023

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

Ein entfernter, authentisierter oder anonym Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonym Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Fri, 20 Oct 2023

[NEU] [hoch] VMware Aria Operations for Logs: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen und Code-Ausführung

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in VMware Aria Operations for Logs ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder beliebigen Code auszuführen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] Red Hat Enterprise Linux (libvpX): Mehrere Schwachstellen

Ein entfernter anonym 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, 20 Oct 2023

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen, Dateien zu manipulieren und beliebigen Programmcode mit den Rechten des Dienstes ausführen zu können.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] Ghostscript: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Ghostscript ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herzustellen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] TLS: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in TLS 1.2 ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in docker ausnutzen, um seine Privilegien zu erhöhen und um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter, anonymmer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] libTIFF: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in libTIFF ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

Ein entfernter, anonymmer oder authentisierter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu verursachen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Fri, 20 Oct 2023

[UPDATE] [hoch] docker: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in docker ausnutzen, um Informationen offenzulegen.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/23/2023	[Ubuntu 16.04 ESM : Bottle vulnerability (USN-5532-2)]	critical
10/23/2023	[Ubuntu 20.04 ESM : Pillow vulnerabilities (USN-5777-2)]	critical
10/23/2023	[Debian DLA-3627-1 : redis - LTS security update]	critical
10/23/2023	[Ubuntu 20.04 LTS : AOM vulnerabilities (USN-6447-1)]	critical
10/23/2023	[Ubuntu 16.04 ESM : Puppet vulnerabilities (USN-4804-1)]	high
10/23/2023	[Ubuntu 16.04 ESM : libjpeg9 vulnerabilities (USN-5336-1)]	high
10/23/2023	[Ubuntu 16.04 ESM : WildMIDI vulnerabilities (USN-4807-1)]	high
10/23/2023	[Ubuntu 16.04 LTS : Firefox vulnerabilities (USN-4278-2)]	high
10/23/2023	[Ubuntu 16.04 ESM : openpyxl vulnerability (USN-4821-1)]	high
10/23/2023	[Ubuntu 16.04 ESM : Libjpeg6b vulnerabilities (USN-5497-2)]	high
10/23/2023	[Ubuntu 20.04 ESM / 22.04 ESM : ldns vulnerabilities (USN-5257-2)]	high
10/23/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6172-1)]	high
10/23/2023	[Ubuntu 20.04 ESM / 22.04 ESM : ImageMagick vulnerabilities (USN-5736-2)]	high
10/23/2023	[Ubuntu 20.04 LTS : Python vulnerabilities (USN-5201-1)]	high
10/23/2023	[Juniper Junos OS Vulnerability (JSA73145)]	high
10/23/2023	[CentOS 8 : varnish (CESA-2023:5989)]	high
10/23/2023	[RHEL 8 : varnish:6 (RHSA-2023:6023)]	high
10/23/2023	[RHEL 8 : varnish:6 (RHSA-2023:6020)]	high
10/23/2023	[RHEL 8 : varnish (RHSA-2023:5989)]	high
10/23/2023	[Oracle Linux 9 : php (ELSA-2023-5926)]	high
10/23/2023	[Oracle Linux 9 : grafana (ELSA-2023-5867)]	high
10/23/2023	[Oracle Linux 8 : nodejs:16 (ELSA-2023-5850)]	high
10/23/2023	[Oracle Linux 8 : grafana (ELSA-2023-5863)]	high
10/23/2023	[Jira Server/Data Center STAGIL Navigation plugin Path Traversal CVE-2023-26256]	high
10/23/2023	[Jira Server/Data Center STAGIL Navigation plugin Path Traversal CVE-2023-26255]	high
10/23/2023	[Debian DLA-3629-1 : ceph - LTS security update]	high
10/23/2023	[Ubuntu 16.04 ESM / 18.04 ESM : libXpm vulnerabilities (USN-6408-2)]	high
10/23/2023	[Ubuntu 18.04 ESM : libvpx vulnerabilities (USN-6403-2)]	high
10/23/2023	[Ubuntu 18.04 ESM : Linux kernel (GCP) vulnerabilities (USN-6441-2)]	high
10/23/2023	[FreeBSD : MySQL – Multiple vulnerabilities (22df5074-71cd-11ee-85eb-84a93843eb75)]	high
10/23/2023	[Trane Tracer Improper Control of Generation of Code (Code Injection) (CVE-2021-38450)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Mon, 23 Oct 2023

Moodle 4.3 Cross Site Scripting

Moodle version 4.3 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 23 Oct 2023

PowerVR Out-Of-Bounds Access / Information Leak

PowerVR suffers from a multitude of memory management bugs including out-of-bounds access and information leakage.

- [Link](#)

” “Fri, 20 Oct 2023

VIMESA VHF/FM Transmitter Blue Plus 9.7.1 Denial Of Service

VIMESA VHF/FM Transmitter Blue Plus version 9.7.1 suffers from a denial of service vulnerability. An unauthenticated attacker can issue an unauthorized HTTP GET request to the unprotected endpoint doreboot and restart the transmitter operations.

- [Link](#)

” “Thu, 19 Oct 2023

Atlassian Confluence Unauthenticated Remote Code Execution

This Metasploit module exploits an improper input validation issue in Atlassian Confluence, allowing arbitrary HTTP parameters to be translated into getter/setter sequences via the XWorks2 middleware and in turn allows for Java objects to be modified at run time. The exploit will create a new administrator user and upload a malicious plugins to get arbitrary code execution. All versions of Confluence between 8.0.0 through to 8.3.2, 8.4.0 through to 8.4.2, and 8.5.0 through to 8.5.1 are affected.

- [Link](#)

” “Wed, 18 Oct 2023

Squid Caching Proxy Proof Of Concepts

Two and a half years ago an independent audit was performed on the Squid Caching Proxy, which ultimately resulted in 55 vulnerabilities being discovered in the project’s C++ source code. Although some of the issues have been fixed, the majority (35) remain valid. The majority have not been assigned CVEs, and no patches or workarounds are available. Some of the listed issues concern more than one bug, which is why 45 issues are listed, despite there being 55 vulnerabilities in total (10 extra of the result of similar, but different pathways to reproduce a vulnerability). After two and a half years of waiting, the researcher has decided to release the issues publicly. This archive contains all of the proof of concept code released by the researcher.

- [Link](#)

” “Tue, 17 Oct 2023

XNSoft Nconvert 7.136 Buffer Overflow / Denial Of Service

XNSoft Nconvert version 7.136 is vulnerable to buffer overflow and denial of service conditions. Proof of concepts included.

- [Link](#)

” “Mon, 16 Oct 2023

NLB mKlik Makedonija 3.3.12 SQL Injection

NLB mKlik Makedonija version 3.3.12 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Mon, 16 Oct 2023

Linux DCCP Information Leak

Linux suffers from a small remote binary information leak in DCCP.

- [Link](#)

” “Mon, 16 Oct 2023

Microsoft Windows Kernel Out-Of-Bounds Reads / Memory Disclosure

The Microsoft Windows Kernel suffers from out-of-bounds reads and paged pool memory disclosure in VrpUp-

dateKeyInformation.

- [Link](#)

” “Mon, 16 Oct 2023

Microsoft Windows Kernel Paged Pool Memory Disclosure

The Microsoft Windows Kernel suffers from a paged pool memory disclosure in VrpPostEnumerateKey.

- [Link](#)

” “Mon, 16 Oct 2023

WordPress Royal Elementor 1.3.78 Shell Upload

WordPress Royal Elementor plugin versions 1.3.78 and below suffer from a remote shell upload vulnerability.

- [Link](#)

” “Mon, 16 Oct 2023

WordPress WP ERP 1.12.2 SQL Injection

WordPress WP ERP plugin versions 1.12.2 and below suffer from a remote SQL injection vulnerability.

- [Link](#)

” “Mon, 16 Oct 2023

ChurchCRM 4.5.4 SQL Injection

ChurchCRM version 4.5.4 suffers from a remote authenticated blind SQL injection vulnerability.

- [Link](#)

” “Mon, 16 Oct 2023

Zoo Management System 1.0 Shell Upload

Zoo Management System version 1.0 suffers from a remote shell upload vulnerability. This version originally had a shell upload vulnerability discovered by D4rkP0w4r that leveraged the upload CV flow but this particular finding leverages the save_animal flow.

- [Link](#)

” “Mon, 16 Oct 2023

2023 Mount Carmel School 6.4.1 Cross Site Scripting

2023 Mount Carmel School version 6.4.1 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 16 Oct 2023

Microsoft Windows Kernel Race Condition / Memory Corruption

The Microsoft Windows Kernel passes user-mode pointers to registry callbacks, leading to race conditions and memory corruption.

- [Link](#)

” “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](#)

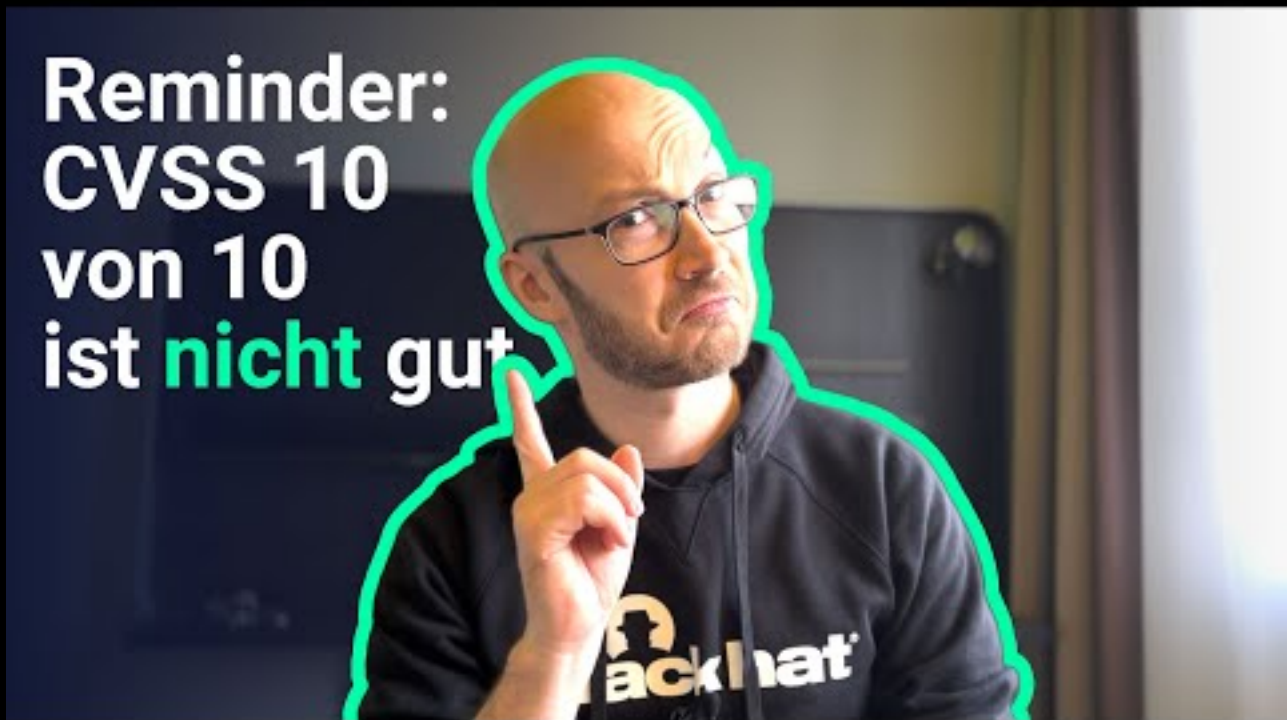
”

0-Day

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
2023-10-20	Museum d'Histoire Naturelle de Berlin	[DEU]	Link
2023-10-20	Westchester Medical Center	[USA]	Link
2023-10-19	Glynn County	[USA]	Link
2023-10-17	La Real Sociedad	[ESP]	Link
2023-10-17	Everi	[USA]	Link
2023-10-16	Psychiatrie Baselland	[CHE]	Link
2023-10-16	Patriotisk Selskab	[DNK]	Link
2023-10-16	Hong Kong Ballet	[HKG]	Link
2023-10-16	La Provincia di Perugia	[ITA]	Link
2023-10-16	Harlingen Police Department	[USA]	Link
2023-10-15	Système judiciaire du Kansas	[USA]	Link
2023-10-15	WMCHealth hospital	[USA]	Link
2023-10-15	American Family Insurance	[USA]	Link
2023-10-14	Henry Schein Inc.	[USA]	Link
2023-10-12	Service Départemental d'Incendie et de Secours des Pyrénées-Atlantiques (SDIS64)	[FRA]	Link
2023-10-11	Akumin	[USA]	Link
2023-10-10	Simpson Manufacturing Co.	[USA]	Link
2023-10-10	Pride of Nottingham (PON)	[GBR]	Link
2023-10-10	Le Cofrac	[FRA]	Link
2023-10-09	De La Salle University (DLSU)	[PHL]	Link
2023-10-09	Kwik Trip	[USA]	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
2023-10-05	Clark County School District (CCSD)	[USA]	Link
2023-10-04	Hochsauerlandenergie et Hochsauerlandwasser	[DEU]	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-Gruppe	Webseite
2023-10-23	[3-D Engineering/ 3-D Precision Machine]	alphv	Link
2023-10-23	[www.portage.k12.in.us]	alphv	Link
2023-10-23	[Newconcepttech]	cuba	Link
2023-10-23	[University of Defence - Full Leak]	monti	Link
2023-10-23	[Penfield Fire Company]	noescape	Link
2023-10-23	[Korea Petroleum Industries Company]	noescape	Link
2023-10-23	[Gasmart Organization]	noescape	Link
2023-10-23	[KBS Accountants, Tax Specialists & Lawyers]	noescape	Link
2023-10-23	[INSTANT ACCESS]	noescape	Link
2023-10-23	[Misterminit]	noescape	Link
2023-10-23	[Central University of Bayamón]	noescape	Link
2023-10-23	[Motorcycles of Charlotte & Greensboro]	noescape	Link
2023-10-23	[International Community Schools]	noescape	Link
2023-10-23	[Order of Psychologists of Lombardy]	noescape	Link
2023-10-23	[Panificio Grandolfo]	blackbasta	Link
2023-10-23	[3-D Engineering]	alphv	Link
2023-10-23	[Safpro]	medusa	Link
2023-10-23	[EHPAD]	medusa	Link
2023-10-23	[Beaver Lake Cree Nation]	medusa	Link
2023-10-23	[Native Counselling Services of Alberta]	medusa	Link
2023-10-23	[Ada-Borup-West School]	medusalocker	Link
2023-10-23	[wellons.org]	medusalocker	Link
2023-10-23	[harlingentx.gov]	lockbit3	Link
2023-10-23	[mamu.be]	lockbit3	Link
2023-10-22	[Ransomedvc Launches A forum]	ransomed	Link
2023-10-22	[Dr. Jaime Schwartz MD, FACS]	hunters	Link
2023-10-22	[Edwards Business Systems]	8base	Link
2023-10-22	[Brunton Shaw]	8base	Link
2023-10-22	[JC Roman Construction]	8base	Link
2023-10-22	[APS - Automotive Parts Solutions]	8base	Link
2023-10-21	[chs.ca]	lockbit3	Link
2023-10-21	[Panetteria Grandolfo]	blackbasta	Link
2023-10-21	[Simpson Strong-Tie]	blackbasta	Link
2023-10-21	[Sidockgroup.]	donutleaks	Link
2023-10-21	[The Law Offices of Julian Lewis Sanders & Associates FULL LEAK!]	alphv	Link
2023-10-20	[Williamson Foodservice]	play	Link
2023-10-20	[Epaccsys]	play	Link
2023-10-20	[Tru-val Electric]	play	Link
2023-10-20	[Bridgeport Fittings]	play	Link
2023-10-20	[Kobi Karp Architecture and Interior Design]	play	Link
2023-10-20	[RADISE]	play	Link
2023-10-20	[Polar Tech Industries]	play	Link
2023-10-20	[Ipswich Bay Glass]	play	Link
2023-10-20	[Hygieneering]	play	Link
2023-10-20	[The Fountain Group]	play	Link
2023-10-20	[Venture Plastics]	play	Link
2023-10-20	[Milk Source]	play	Link
2023-10-20	[We Hire Pentesters(5BTC Payout)]	ransomed	Link
2023-10-20	[uaes.com]	lockbit3	Link
2023-10-20	[degrootgroep.nl]	lockbit3	Link
2023-10-20	[charleystaxi.com]	lockbit3	Link
2023-10-12	[UK Stratton Primary School]	hunters	Link
2023-10-20	[Royal College of Physicians and Surgeonsof Glasgow]	akira	Link
2023-10-20	[Southland IntegratedServices]	akira	Link
2023-10-20	[Protector Fire Services]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-20	[kvc constructors inc]	alphv	Link
2023-10-19	[Superline - Full Leak]	monti	Link
2023-10-19	[Government of Brazil - Business Information Brazil]	blacksuit	Link
2023-10-19	[Associated Wholesale Grocers]	play	Link
2023-10-19	[Visionary Integration Professionals]	akira	Link
2023-10-19	[Inventum Øst]	akira	Link
2023-10-19	[nirolaw.com]	lockbit3	Link
2023-10-19	[QuadraNet Enterprises]	akira	Link
2023-10-19	[hgmonline.com]	lockbit3	Link
2023-10-19	[salaw.com]	lockbit3	Link
2023-10-19	[frs-fnrs.be]	lockbit3	Link
2023-10-19	[thecsi.com]	lockbit3	Link
2023-10-19	[smart-union.org]	lockbit3	Link
2023-10-19	[Innovattel LLC]	alphv	Link
2023-10-19	[CADRE]	alphv	Link
2023-10-18	[fdf.org]	lockbit3	Link
2023-10-18	[Dow Golub Remels & Gilbreath]	bianlian	Link
2023-10-18	[Griffing & Company, P.C]	bianlian	Link
2023-10-18	[International Biomedical Ltd]	bianlian	Link
2023-10-18	[Jebsen & Co. Ltd.]	bianlian	Link
2023-10-12	[KBS Accountants]	noescape	Link
2023-10-17	[Rotorcraft Leasing Company]	0mega	Link
2023-10-17	[Catarineau & Givens P.A. FULL LEAK!]	alphv	Link
2023-10-17	[kasperekusaoptical.com]	lockbit3	Link
2023-10-17	[SIIX Corporation]	alphv	Link
2023-10-17	[STANTON WILLIAMS]	blackbasta	Link
2023-10-17	[Edwardian Hotels London]	blackbasta	Link
2023-10-17	[HAFFNER GmbH Co.]	blackbasta	Link
2023-10-17	[Intred]	blackbasta	Link
2023-10-17	[Ampersand]	blackbasta	Link
2023-10-17	[BACCARAT]	blackbasta	Link
2023-10-17	[PIEMME S.p.A.]	blackbasta	Link
2023-10-17	[Greenpoint]	incransom	Link
2023-10-09	[Gasmart]	noescape	Link
2023-10-16	[cpstate.org]	lockbit3	Link
2023-10-16	[ATI Traduction]	medusa	Link
2023-10-16	[EDB]	medusa	Link
2023-10-16	[Global Product Sales]	medusa	Link
2023-10-16	[Symposia Organizzazione Congressi S.R.L]	medusa	Link
2023-10-16	[sdproducts.co.uk]	lockbit3	Link
2023-10-16	[SCS SpA]	cactus	Link
2023-10-16	[OmniVision Technologies]	cactus	Link
2023-10-16	[Believe Productions]	medusa	Link
2023-10-16	[Ransomedvc Pentest Services!]	ransomed	Link
2023-10-09	[Mount Holly Nissan]	noescape	Link
2023-10-16	[Boise Rescue Mission Ministries]	alphv	Link
2023-10-16	[DOMAIN-BACCARAT_2]	blackbasta	Link
2023-10-16	[NCC_2]	blackbasta	Link
2023-10-16	[RE : Clarification]	ransomed	Link
2023-10-16	[Rob Lee Evidence : Sneak Peek]	ransomed	Link
2023-10-16	[Cogal Industry]	snatch	Link
2023-10-15	[Islamic Azad University Electronic Campus]	arvinclub	Link
2023-10-15	[Colonial Pipeline Company]	ransomed	Link
2023-10-15	[Accenture Breach Evidence & Debunking Rob Lee's Lies]	ransomed	Link
2023-10-15	[webpag.com.br database leaked]	ransomed	Link
2023-10-15	[QSI INC - Credit Cards & Transaction Processing]	alphv	Link
2023-10-14	[DUHOCAAU]	mallox	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-14	[The Law Offices of Julian Lewis Sanders & Associates]	alphv	Link
2023-10-14	[Jaresh Innovation]	arvinclub	Link
2023-10-14	[Northwest Eye Care Professionals]	rhysida	Link
2023-10-14	[Intech]	snatch	Link
2023-10-13	[Catholic Charities]	incransom	Link
2023-10-13	[Kimia Tadbir Kiyani]	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

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-10	[mountstmarys]	cuba	Link
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	[vsmpto-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

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-05	[RICOR Global Limited]	cactus	Link
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.