



Ausgabe: 20230909

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

NSO-Group-Angriff: Notfall-Updates für iPhone, iPad, Mac und Apple Watch

Apple hat am Donnerstagabend nochmals Updates für seine aktuellen Betriebssysteme nachgeschoben. Enthalten sind Fixes für einen aktiven Exploit.

- [Link](#)

Aruba-Controller und -Gateways mit hochriskanten Sicherheitslücken

Für Aruba-Controller und -Gateways der Serien 9000 und 9200 gibt es Updates, die hochriskante Sicherheitslücken schließen.

- [Link](#)

Sicherheitsupdates: Unbefugte Zugriffe auf TP-Link-Router möglich

Angreifer können verschiedene Router von TP-Link attackieren und im schlimmsten Fall eigene Befehle auf Geräten ausführen.

- [Link](#)

Cisco warnt vor teils kritischen Lücken und liefert Updates für mehrere Produkte

In mehreren Cisco-Produkten lauern Sicherheitslücken, die Updates schließen sollen. Eine gilt sogar als kritisch.

- [Link](#)

Patchday: Schadcode-Attacken auf Android 11, 12, 13 möglich

Google und weitere Hersteller von Android-Geräten haben wichtige Sicherheitsupdates veröffentlicht. Eine Lücke wird bereits ausgenutzt.

- [Link](#)

Sicherheitsupdates: Angreifer können Kontrolle über Asus-Router erlangen

Mehrere Sicherheitslücken gefährden verschiedene Router-Modelle von Asus. Patches sichern Geräte ab.

- [Link](#)

Webbrowser: Hochriskante Schwachstellen in Google Chrome geschlossen

Google stopft mit aktualisierten Chrome-Versionen vier als hochriskant eingestufte Sicherheitslücken.

- [Link](#)

AVM: Fritzbox-Firmware 7.57 und 7.31 stoppen Sicherheitsleck

AVM hat für zahlreiche Fritzboxen die Firmware 7.57 und 7.31 veröffentlicht. Es handelt sich um Stabilitäts- und Sicherheitsupdates.

- [Link](#)

Jetzt aktualisieren! Proof-of-Concept für kritische VMware-Aria-Lücke

Vergangene Woche hat VMware Updates zum Schließen einer kritischen Sicherheitslücke herausgegeben. Jetzt ist ein Proof-of-Concept verfügbar. Zeit fürs Update!

- [Link](#)

Kritische Lücke in VPN von Securepoint

Updates sollen eine kritische Sicherheitslücke in der VPN-Software von Securepoint schließen, durch die Angreifer ihre Rechte ausweiten können.

- [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	0.985780000	Link
CVE-2023-38035	0.960130000	0.992550000	Link
CVE-2023-3519	0.911990000	0.984910000	Link
CVE-2023-35078	0.965240000	0.994210000	Link
CVE-2023-34362	0.936790000	0.987850000	Link
CVE-2023-33246	0.971460000	0.997000000	Link
CVE-2023-32315	0.973420000	0.998280000	Link
CVE-2023-28771	0.917110000	0.985320000	Link
CVE-2023-28121	0.937820000	0.987950000	Link
CVE-2023-27372	0.970600000	0.996560000	Link
CVE-2023-27350	0.970860000	0.996700000	Link
CVE-2023-26469	0.910820000	0.984790000	Link
CVE-2023-26360	0.908440000	0.984530000	Link
CVE-2023-25717	0.965660000	0.994440000	Link
CVE-2023-25194	0.924830000	0.986160000	Link
CVE-2023-24489	0.974410000	0.999140000	Link
CVE-2023-21839	0.960800000	0.992740000	Link
CVE-2023-21823	0.907830000	0.984490000	Link
CVE-2023-21554	0.954850000	0.991290000	Link
CVE-2023-20887	0.960660000	0.992690000	Link
CVE-2023-0669	0.965780000	0.994480000	Link

BSI - Warn- und Informationsdienst (WID)

Fri, 08 Sep 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](#)

Fri, 08 Sep 2023

[NEU] [hoch] IBM Maximo Asset Management: Mehrere Schwachstellen

Ein entfernter, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in IBM Maximo Asset Management ausnutzen, um beliebigen Programmcode auszuführen, einen Cross-Site Scripting Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Oracle Linux ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Apache Kafka: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Apache Kafka ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, Informationen offenzulegen, seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um Administratorrechte zu erlangen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Apple iOS/iPadOS: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um Administratorrechte zu erlangen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

Ein entfernter, anonym oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

Fri, 08 Sep 2023

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonym, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Apple macOS

ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und seine Privilegien zu erweitern.

- [Link](#)

Fri, 08 Sep 2023

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

Ein entfernter, anonymen 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](#)

Fri, 08 Sep 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](#)

Fri, 08 Sep 2023

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

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- [Link](#)

Fri, 08 Sep 2023

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

Ein entfernter anonymen Angreifer kann diese Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen und Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

Fri, 08 Sep 2023

[NEU] [kritisch] Apple macOS: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Apple macOS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Fri, 08 Sep 2023

[NEU] [kritisch] Apple iOS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Thu, 07 Sep 2023

[NEU] [hoch] ArubaOS: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Aruba ArubaOS ausnutzen, um Sicherheitsvorkehrungen zu umgehen und das System komplett zu kompromittieren.

- [Link](#)

Thu, 07 Sep 2023

[NEU] [hoch] Jenkins Plugins: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Jenkins Plugins ausnutzen, um Dateien zu manipulieren, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

Thu, 07 Sep 2023

[NEU] [hoch] MinIO: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in MinIO ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/8/2023	[Amazon Linux 2 : ca-certificates (ALAS-2023-2224)]	critical
9/8/2023	[Amazon Linux 2 : sox (ALAS-2023-2231)]	critical
9/8/2023	[Amazon Linux 2023 : php8.1, php8.1-bcmath, php8.1-cli (ALAS2023-2023-325)]	critical
9/8/2023	[Amazon Linux 2023 : php8.2, php8.2-bcmath, php8.2-cli (ALAS2023-2023-324)]	critical
9/8/2023	[Ubuntu 20.04 LTS / 22.04 LTS : GRUB2 vulnerabilities (USN-6355-1)]	critical
9/8/2023	[Oracle Linux 8 : istio (ELSA-2023-12780)]	critical
9/8/2023	[Oracle Linux 7 : istio (ELSA-2023-12781)]	critical
9/8/2023	[Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-6339-2)]	critical
9/8/2023	[GLSA-202309-01 : Apache HTTPD: Multiple Vulnerabilities]	critical
9/8/2023	[Amazon Linux 2023 : postgresql15, postgresql15-contrib, postgresql15-llvmjit (ALAS2023-2023-322)]	high
9/8/2023	[Amazon Linux 2023 : clamav, clamav-data, clamav-devel (ALAS2023-2023-331)]	high
9/8/2023	[Amazon Linux 2 : kernel (ALAS-2023-2232)]	high
9/8/2023	[Amazon Linux 2 : rust (ALAS-2023-2223)]	high
9/8/2023	[Amazon Linux 2 : amazon-ssm-agent (ALAS-2023-2238)]	high
9/8/2023	[Amazon Linux 2023 : aspnetcore-runtime-6.0, aspnetcore-targeting-pack-6.0, dotnet (ALAS2023-2023-326)]	high
9/8/2023	[Amazon Linux 2 : ImageMagick (ALAS-2023-2239)]	high
9/8/2023	[Amazon Linux 2023 : krb5-devel, krb5-libs, krb5-pkinit (ALAS2023-2023-321)]	high
9/8/2023	[Amazon Linux 2023 : binutils, binutils-devel, binutils-gprofng (ALAS2023-2023-334)]	high
9/8/2023	[Amazon Linux 2 : curl (ALAS-2023-2230)]	high
9/8/2023	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2023-330)]	high
9/8/2023	[Amazon Linux 2 : clamav (ALAS-2023-2233)]	high
9/8/2023	[Amazon Linux 2023 : python3.11, python3.11-devel, python3.11-idle (ALAS2023-2023-317)]	high
9/8/2023	[Amazon Linux 2023 : gdk-pixbuf2, gdk-pixbuf2-devel, gdk-pixbuf2-modules (ALAS2023-2023-341)]	high
9/8/2023	[Amazon Linux 2023 : amazon-ecr-credential-helper (ALAS2023-2023-337)]	high
9/8/2023	[Amazon Linux 2 : ImageMagick (ALAS-2023-2240)]	high
9/8/2023	[Amazon Linux 2023 : cargo, clippy, rust (ALAS2023-2023-323)]	high
9/8/2023	[Debian DLA-3558-1 : python-django - LTS security update]	high
9/8/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6340-2)]	high
9/8/2023	[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel (Azure) (USN-6342-2)]	high
9/8/2023	[Debian DLA-3559-1 : libssh2 - LTS security update]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Fri, 08 Sep 2023

WinRAR Remote Code Execution

This Metasploit module exploits a vulnerability in WinRAR (CVE-2023-38831). When a user opens a crafted RAR file and its embedded document, the decoy document is executed, leading to code execution.

- [Link](#)

” “Fri, 08 Sep 2023

LG Simple Editor Remote Code Execution

This Metasploit module exploits broken access control and directory traversal vulnerabilities in LG Simple Editor software for gaining code execution. The vulnerabilities exist in versions of LG Simple Editor prior to v3.21. By exploiting this flaw, an attacker can upload and execute a malicious JSP payload with the SYSTEM user permissions.

- [Link](#)

” “Fri, 08 Sep 2023

Sonicwall GMS 9.9.9320 Remote Code Execution

This Metasploit module exploits a series of vulnerabilities - including auth bypass, SQL injection, and shell injection - to obtain remote code execution on SonicWall GMS versions 9.9.9320 and below.

- [Link](#)

” “Fri, 08 Sep 2023

OpenTSDB 2.4.1 Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in the key parameter in OpenTSDB through 2.4.1 in order to achieve unauthenticated remote code execution as the root user. The module first attempts to obtain the OpenTSDB version via the api. If the version is 2.4.1 or lower, the module performs additional checks to obtain the configured metrics and aggregators. It then randomly selects one metric and one aggregator and uses those to instruct the target server to plot a graph. As part of this request, the key parameter is set to the payload, which will then be executed by the target if the latter is vulnerable. This module has been successfully tested against OpenTSDB version 2.4.1.

- [Link](#)

” “Fri, 08 Sep 2023

Kibana Timelion Prototype Pollution Remote Code Execution

Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This leads to an arbitrary command execution with permissions of the Kibana process on the host system. Exploitation will require a service or system reboot to restore normal operation. The WFSDELAY parameter is crucial for this exploit. Setting it too high will cause MANY shells (50-100+), while setting it too low will cause no shells to be obtained. WFSDELAY of 10 for a docker image caused 6 shells.

- [Link](#)

” “Fri, 08 Sep 2023

Microsoft Windows Kernel Recovery Memory Corruption

The Microsoft Windows Kernel has an issue where a partial success of registry hive log recovery may lead to inconsistent state and memory corruption.

- [Link](#)

” “Fri, 08 Sep 2023

Microsoft Windows Kernel Integer Overflow / Out-Of-Bounds Read

The Microsoft Windows Kernel suffers from out-of-bounds reads due to an integer overflow in registry .LOG file parsing.

- [Link](#)

” “Fri, 08 Sep 2023

Event Ticketing System 1.0 Cross Site Scripting

Event Ticketing System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

SyncBreeze 15.2.24 Denial Of Service

SyncBreeze version 15.2.24 suffers from a denial of service vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

GOM Player 2.3.90.5360 Buffer Overflow

GOM Player version 2.3.90.5360 suffers from a buffer overflow vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

Drupal 10.1.2 Web Cache Poisoning

Drupal version 10.1.2 appears to suffer from web cache poisoning due to a server-side request forgery vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

Wp2Fac 1.0 Command Injection

Wp2Fac version 1.0 suffers from an OS command injection vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

TECHView LA5570 Wireless Gateway 1.0.19_T53 Traversal / Privilege Escalation

TECHView LA5570 Wireless Gateway version 1.0.19_T53 suffers from directory traversal, privilege escalation, and information disclosure vulnerabilities.

- [Link](#)

” “Fri, 08 Sep 2023

Soosyze 2.0.0 Arbitrary File Upload

Soosyze version 2.0.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

Axigen 10.5.0-4370c946 Cross Site Scripting

Axigen versions 10.5.0-4370c946 and below suffer from a cross site scripting vulnerability.

- [Link](#)

” “Fri, 08 Sep 2023

WordPress Elementor Iframe Injection

WordPress Elementor plugin versions prior to 3.5.5 suffer from an iframe injection vulnerability.

- [Link](#)

” “Thu, 07 Sep 2023

JPC2 CMS 1.0 SQL Injection

JPC2 CMS version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Thu, 07 Sep 2023

Izdelava IDS 2.0 Cross Site Scripting

Izdelava IDS version 2.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Thu, 07 Sep 2023

Meeting Room Booking System 1.0 SQL Injection

Meeting Room Booking System version 1.0 suffers from multiple remote SQL injection vulnerabilities.

- [Link](#)

” “Wed, 06 Sep 2023

SolarView Compact 6.00 Remote Command Execution

This Metasploit module exploits a command injection vulnerability on the SolarView Compact version 6.00 web

application via the vulnerable endpoint downloader.php. After exploitation, an attacker will have full access with the same user privileges under which the webserver is running (typically as user contec).

- [Link](#)

” “Wed, 06 Sep 2023

WordPress Newsletter 7.8.9 Cross Site Scripting

WordPress Newsletter plugin versions 7.8.9 and below suffer from a persistent cross site scripting vulnerability.

- [Link](#)

” “Wed, 06 Sep 2023

Microsoft Windows Privilege Escalation

Windows still suffers from issues related to the replacement of the system drive letter during impersonation. This can be abused to trick privilege processes to load configuration files and other resources from untrusted locations leading to elevation of privilege.

- [Link](#)

” “Wed, 06 Sep 2023

OpenCart CMS 4.0.2.2 Brute Force

OpenCart CMS version 4.0.2.2 suffers from a login brute forcing vulnerability.

- [Link](#)

” “Wed, 06 Sep 2023

Cleaning Business Software 1.0 Cross Site Scripting

Cleaning Business Software version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Wed, 06 Sep 2023

Event Booking Calendar 4.0 Cross Site Scripting

Event Booking Calendar version 4.0 suffers from a cross site scripting vulnerability.

- [Link](#)

”

0-Day

“Fri, 08 Sep 2023

ZDI-23-1400: Delta Electronics CNCSoft-B DPA File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1399: Visualware MyConnection Server doRTAAccessCTConfig Cross-Site Scripting Authentication Bypass Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1398: Visualware MyConnection Server doRTAAccessUPass Exposed Dangerous Method Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1397: Visualware MyConnection Server doIForward XML External Entity Processing Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1396: Visualware MyConnection Server doPostUploadfiles Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1395: Kofax Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1394: Kofax Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1393: Kofax Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1392: Kofax Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1391: PDF-XChange Editor mailForm Use-After-Free Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1390: PDF-XChange Editor JPG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1389: PDF-XChange Editor EMF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1388: PDF-XChange Editor EMF File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1387: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1386: PDF-XChange Editor JPG File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1385: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1384: PDF-XChange Editor JPG File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1383: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1382: PDF-XChange Editor EMF File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1381: PDF-XChange Editor JP2 File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1380: PDF-XChange Editor J2K File Parsing Uninitialized Variable Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1379: PDF-XChange Editor EMF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1378: PDF-XChange Editor JPG File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1377: PDF-XChange Editor PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1376: PDF-XChange Editor addScript Type Confusion Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1375: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1374: PDF-XChange Editor Doc Object Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1373: PDF-XChange Editor JPC File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1372: PDF-XChange Editor Doc Object Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1371: PDF-XChange Editor PDF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1370: PDF-XChange Editor PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1369: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1368: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1367: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1366: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1365: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1364: PDF-XChange Editor U3D File Parsing Uninitialized Variable Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1363: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1362: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1361: PDF-XChange Editor U3D File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1360: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1359: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1358: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1357: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1356: PDF-XChange Editor Annotation Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1355: PDF-XChange Editor App Object Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1354: PDF-XChange Editor J2K File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1353: PDF-XChange Editor J2K File Parsing Uninitialized Variable Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1352: PDF-XChange Editor JP2 File Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1351: PDF-XChange Editor J2K File Parsing Uninitialized Variable Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1350: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1349: PDF-XChange Editor EMF File Parsing Use-After-Free Information Disclosure Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1348: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1347: PDF-XChange Editor U3D File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 08 Sep 2023

ZDI-23-1346: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

"Fri, 08 Sep 2023

ZDI-23-1345: PDF-XChange Editor JP2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

"Fri, 08 Sep 2023

ZDI-23-1344: PDF-XChange Editor J2K File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

"Fri, 08 Sep 2023

ZDI-23-1343: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1342: Synology RT6600ax info.cgi Exposure of Sensitive Data Information Disclosure Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1341: Synology RT6600ax uistrings.cgi Path Traversal Information Disclosure Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1340: Synology RT6600ax SYNO.Core Uncontrolled Resource Consumption Denial-of-Service Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1339: Synology RT6600ax WEB API Endpoint Command Injection Remote Code Execution Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1338: D-Link DIR-3040 HTTP Request Processing Referer Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1337: D-Link DIR-3040 HTTP Request Processing Referer Heap-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1336: D-Link DIR-3040 prog.cgi SetUsersSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1335: D-Link DIR-3040 prog.cgi SetTriggerPPPoEValidate Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

"Thu, 07 Sep 2023

ZDI-23-1334: D-Link DIR-3040 prog.cgi SetMyDLinkRegistration Stack-Based Buffer Overflow

Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1333: D-Link DIR-3040 prog.cgi SetIPv6PppoeSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1332: D-Link DIR-3040 prog.cgi SetDeviceSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1331: D-Link DIR-3040 prog.cgi SetQuickVPNSettings PSK Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1330: D-Link DIR-3040 prog.cgi SetWan2Settings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1329: D-Link DIR-3040 prog.cgi SetWlanRadioSecurity Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1328: D-Link DIR-3040 prog.cgi SetSysEmailSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1327: D-Link DIR-3040 prog.cgi SetWanSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1326: D-Link DIR-3040 prog.cgi SetWan3Settings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1325: D-Link DIR-3040 prog.cgi SetQuickVPNSettings Password Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1324: D-Link DIR-3040 prog.cgi SetDynamicDNSSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1323: D-Link DAP-1325 CGI Missing Authentication Information Disclosure Vulnerability

- [Link](#)

" "Thu, 07 Sep 2023

ZDI-23-1322: D-Link DAP-1325 HNAP Missing Authentication Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1321: D-Link DAP-1325 setDhcpAssignRangeUpdate lan_ipaddr Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1320: D-Link DAP-1325 SetTriggerAPValidate Key Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1319: D-Link DAP-1325 SetHostIPv6StaticSettings StaticPrefixLength Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1318: D-Link DAP-1325 SetHostIPv6StaticSettings StaticDNS2 Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1317: D-Link DAP-1325 SetHostIPv6StaticSettings StaticDNS1 Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1316: D-Link DAP-1325 SetHostIPv6StaticSettings StaticDefaultGateway Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1315: D-Link DAP-1325 SetHostIPv6StaticSettings StaticAddress Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1314: D-Link DAP-1325 SetHostIPv6Settings IPv6Mode Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1313: D-Link DAP-1325 SetAPLanSettings SubnetMask Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1312: D-Link DAP-1325 SetAPLanSettings SecondaryDNS Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1311: D-Link DAP-1325 SetAPLanSettings PrimaryDNS Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1310: D-Link DAP-1325 SetAPLanSettings Mode Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1309: D-Link DAP-1325 H NAP SetSetupWizardStatus Enabled Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1308: D-Link DAP-1325 H NAP SetHostIPv6StaticSettings StaticPrefixLength Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1307: D-Link DAP-1325 H NAP SetHostIPv6StaticSettings StaticDNS2 Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1306: D-Link DAP-1325 H NAP SetHostIPv6StaticSettings StaticDNS1 Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1305: D-Link DAP-1325 H NAP SetHostIPv6StaticSettings StaticDefaultGateway Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1304: D-Link DAP-1325 H NAP SetHostIPv6StaticSettings StaticAddress Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1303: D-Link DAP-1325 H NAP SetHostIPv6Settings IPv6Mode Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1302: D-Link DAP-1325 H NAP SetAPLanSettings SubnetMask Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1301: D-Link DAP-1325 H NAP SetAPLanSettings SecondaryDNS Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1300: D-Link DAP-1325 H NAP SetAPLanSettings PrimaryDNS Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1299: D-Link DAP-1325 H NAP SetAPLanSettings Mode Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1298: D-Link DAP-1325 H NAP SetAPLanSettings IPAddr Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1297: D-Link DAP-1325 HNAP SetAPLanSettings Gateway Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1296: D-Link DAP-1325 HNAP SetAPLanSettings DeviceName Command Injection Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 07 Sep 2023

ZDI-23-1295: D-Link DAP-1325 setDhcpAssignRangeUpdate lan_ipaddr Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

”

Die Hacks der Woche

mit Martin Haunschmid

NEIN NICHT DIE PAW PATROL & Qakbot Takedown



[Zum Youtube Video](#)

Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2023-09-07	Le groupe hospitalier Saint-Vincent à Strasbourg	[FRA]	Link
2023-09-06	L'académie St Augustine à Maidstone	[GBR]	Link
2023-09-05	Mairie de Séville	[ESP]	Link
2023-09-05	Financial Services Commission (FSC)	[JAM]	Link
2023-09-04	Maiden Erlegh Trust	[GBR]	Link
2023-09-04	Abdelmalek Essaadi University	[MAR]	Link
2023-09-01	Comitato Elettrotecnico Italiano (CEI)	[ITA]	Link
2023-09-01	Secrétariat de l'environnement et des ressources naturelles (Semarnat)	[MEX]	Link

Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-08	[www.northriverco.com]	abyss	Link
2023-09-08	[sd69.org]	lockbit3	Link
2023-09-08	[milbermakris.com]	lockbit3	Link
2023-09-08	[monaco-technologies.com]	lockbit3	Link
2023-09-08	[UNIVERSAL REALTY GROUP]	8base	Link
2023-09-08	[Geo Tek]	cactus	Link
2023-09-08	[hanwha.com]	lockbit3	Link
2023-09-08	[Custom Powder Systems]	cactus	Link
2023-09-08	[JSS Almonds]	cactus	Link
2023-09-08	[atWork Office Furniture]	cactus	Link
2023-09-08	[BRiC Partnership]	cactus	Link
2023-09-08	[PAUL-ALEXANDRE DOICESCO]	qilin	Link
2023-09-08	[WACOAL]	qilin	Link
2023-09-08	[Linktera]	ransomed	Link
2023-09-07	[24/7 Express Logistics]	ragroup	Link
2023-09-07	[FOCUS Business Solutions]	blackbyte	Link
2023-09-07	[Chambersburg Area School District]	blackbyte	Link
2023-09-07	[Pvc-ms]	stormous	Link
2023-09-07	[toua.net]	lockbit3	Link
2023-09-07	[Conselho Superior da Justiça do Trabalho]	8base	Link
2023-09-07	[Sebata Holdings (MICROmega Holdings)]	bianlian	Link
2023-09-07	[TORMAX USA]	cactus	Link
2023-09-07	[West Craft Manufacturing]	cactus	Link
2023-09-07	[Trimaran Capital Partners]	cactus	Link
2023-09-07	[Specialised Management Services]	cactus	Link
2023-09-06	[nobleweb.com]	lockbit3	Link
2023-09-06	[protosign.it]	lockbit3	Link
2023-09-06	[concrejato.com.br]	lockbit3	Link
2023-09-06	[meroso.be]	lockbit3	Link
2023-09-06	[qsoftnet.com]	lockbit3	Link
2023-09-06	[ragasa.com.mx]	lockbit3	Link
2023-09-06	[I Keating Furniture World]	incransom	Link
2023-09-06	[onyx-fire.com]	lockbit3	Link
2023-09-06	[gormanusa.com]	lockbit3	Link
2023-09-06	[Israel Medical Center - leaked]	ragnarlocker	Link
2023-09-06	[It4 Solutions Robras]	incransom	Link
2023-09-06	[Smead]	blackbyte	Link
2023-09-06	[Solano-Napa Pet Emergency Clinic]	knight	Link
2023-09-06	[Ayass BioScience]	alphv	Link
2023-09-06	[Sabre Corporation]	dunghill_leak	Link
2023-09-06	[Energy One]	akira	Link
2023-09-06	[FRESH TASTE PRODUCE USA AND ASSOCIATES INC.]	8base	Link
2023-09-06	[Chula Vista Electric (CVE)]	8base	Link
2023-09-05	[Precisely, Winshuttle]	play	Link
2023-09-05	[Kikkerland Design]	play	Link
2023-09-05	[Markentrainer Werbeagentur]	play	Link
2023-09-05	[Master Interiors]	play	Link
2023-09-05	[Bordelon Marine]	play	Link
2023-09-05	[Majestic Spice]	play	Link
2023-09-04	[Infinity Construction Company]	noescape	Link
2023-09-05	[Maxxd Trailers]	cactus	Link
2023-09-05	[MINEMAN Systems]	cactus	Link
2023-09-05	[Promotrans]	cactus	Link
2023-09-05	[Seymours]	cactus	Link
2023-09-02	[Strata Plan Australia FULL LEAK]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-02	[TissuPath Australia FULL LEAK]	alphv	Link
2023-09-05	[Marfrig Global Foods]	cactus	Link
2023-09-05	[Brooklyn Premier Orthopedics FULL LEAK!]	alphv	Link
2023-09-05	[Barry Plant LEAK!]	alphv	Link
2023-09-05	[Barsco]	cactus	Link
2023-09-05	[Feroni SPA]	cactus	Link
2023-09-05	[Hornslyd Købmandsgaard]	cactus	Link
2023-09-05	[Lagarde Meregnani]	cactus	Link
2023-09-05	[spmbllaw.com]	lockbit3	Link
2023-09-05	[Unimed]	trigona	Link
2023-09-05	[Cyberport]	trigona	Link
2023-09-05	[godbeylaw.com]	lockbit3	Link
2023-09-01	[Firmdale Hotels]	play	Link
2023-09-04	[easydentalcare.us]	ransomed	Link
2023-09-04	[quantinuum.com]	ransomed	Link
2023-09-04	[laasr.eu]	ransomed	Link
2023-09-04	[medcenter-tambov.ru]	ransomed	Link
2023-09-04	[makflix.eu]	ransomed	Link
2023-09-04	[nucleus.live]	ransomed	Link
2023-09-04	[wantager.com]	ransomed	Link
2023-09-04	[Zurvita]	ragroup	Link
2023-09-04	[Piex Group]	ragroup	Link
2023-09-04	[Yuxin Automobile Co.Ltd ()]	ragroup	Link
2023-09-02	[Mulkay Cardiology Consultants]	noescape	Link
2023-09-04	[Balcan]	cactus	Link
2023-09-04	[Barco Uniforms]	cactus	Link
2023-09-04	[Swipe.bg]	ransomed	Link
2023-09-04	[Balmitt Bulgaria]	ransomed	Link
2023-09-04	[cdwg.com]	lockbit3	Link
2023-09-04	[Betton France]	medusa	Link
2023-09-04	[Jules B]	medusa	Link
2023-09-04	[VVandA]	8base	Link
2023-09-04	[Prodegest Assessors]	8base	Link
2023-09-04	[Knight Barry Title]	snatch	Link
2023-09-03	[phms.com.au]	ransomed	Link
2023-09-03	[paynesvilleareainsurance.com]	ransomed	Link
2023-09-03	[SKF.com]	ransomed	Link
2023-09-03	[gossilaw.com]	lockbit3	Link
2023-09-03	[marianoshoes.com]	lockbit3	Link
2023-09-03	[Arkopharma]	incransom	Link
2023-09-02	[Taylor University]	moneymessage	Link
2023-09-03	[Riverside Logistics]	moneymessage	Link
2023-09-03	[Estes Design & Manufacturing]	moneymessage	Link
2023-09-03	[Aiphone]	moneymessage	Link
2023-09-03	[DDB Unlimited (ddbunlimited.com)]	rancoz	Link
2023-09-03	[Rick Ramos Law (rickramoslaw.com)]	rancoz	Link
2023-09-03	[Newton Media A.S]	alphv	Link
2023-09-03	[Lawsonlundell]	alphv	Link
2023-09-02	[glprop.com]	lockbit3	Link
2023-09-02	[Strata Plan Australia]	alphv	Link
2023-09-02	[TissuPath Australia]	alphv	Link
2023-09-02	[seasonsdarlingharbour.com.au]	lockbit3	Link
2023-09-02	[nerolac.com]	lockbit3	Link
2023-09-02	[ramlowstein.com]	lockbit3	Link
2023-09-02	[Barry Plant Real Estate Australia]	alphv	Link
2023-09-02	[sterncoengineers.com]	lockbit3	Link
2023-09-02	[attorneydanwinder.com]	lockbit3	Link
2023-09-02	[designlink.us]	lockbit3	Link
2023-09-02	[gh2.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-09-02	[DOIT - Canadian IT company allowed leak of its own clients.]	ragnarlocker	Link
2023-09-02	[SKF.com]	everest	Link
2023-09-02	[Powersportsmarketing.com]	everest	Link
2023-09-02	[Statefarm.com]	everest	Link
2023-09-02	[Aban Tether & OK exchange]	arvinclub	Link
2023-09-02	[cc-gorgesardeche.fr]	lockbit3	Link
2023-09-01	[cciamp.com]	lockbit3	Link
2023-09-01	[Templeman Consulting Group Inc]	bianlian	Link
2023-09-01	[vodatech.com.tr]	lockbit3	Link
2023-09-01	[F??????? ?????s]	play	Link
2023-09-01	[Hawaii Health System]	ransomed	Link
2023-09-01	[hamilton-techservices.com]	lockbit3	Link
2023-09-01	[aquinas.qld.edu.au]	lockbit3	Link
2023-09-01	[konkconsulting.com]	lockbit3	Link
2023-09-01	[Piex Group]	ragroup	Link
2023-09-01	[Yuxin Automobile Co.Ltd()]	ragroup	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.