



Ausgabe: 20231229

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

Kritische Sicherheitslücke in Perl-Bibliothek: Schwachstelle bereits ausgenutzt

In einer Perl-Bibliothek zum Parsen von Excel-Dateien haben Sicherheitsforscher eine kritische Schwachstelle entdeckt, die Angreifer bereits ausgenutzt haben.

- [Link](#)

Kritische Lücken in Mobile-Device-Management-Lösung Ivanti Avalanche geschlossen

Angreifer können Ivanti Avalanche mit Schadcode attackieren. Eine reparierte Version steht zum Download bereit.

- [Link](#)

Google Chrome: Zero-Day-Lücke wird angegriffen, Update verfügbar

Googles Entwickler haben ein Update für Chrome veröffentlicht, das eine bereits angegriffene Sicherheitslücke abdichtet.

- [Link](#)

Firefox und Thunderbird: Sicherheitslücken geschlossen und Funktionen ergänzt

Die neuen Versionen von Firefox und Thunderbird dichten Sicherheitslecks ab. Zudem bringen sie neue Funktionen mit.

- [Link](#)

Jetzt patchen! Botnetz InfectedSlurs hat es auf Qnap NAS abgesehen

Eine Sicherheitslücke in der IP-Kamera-Software VioStor NVR auf Netzwerkspeichern von Qnap dient als Schlupfloch für Malware.

- [Link](#)

Sicherheitsupdates: Fortinet schützt Firewalls & Co. vor möglichen Attacken

Der Netzwerkausrüster Fortinet hat in mehreren Produkten gefährliche Lücken geschlossen.

- [Link](#)

Squid-Proxy: Denial of Service durch Endlosschleife

Schickt ein Angreifer einen präparierten HTTP-Header an den Proxy-Server, kann er ihn durch eine unkontrollierte Rekursion zum Stillstand bringen.

- [Link](#)

Zoom behebt Sicherheitslücken unter Windows, Android und iOS

Durch ungenügende Zugriffskontrolle, Verschlüsselungsprobleme und Pfadmanipulation konnten Angreifer sich zusätzliche Rechte verschaffen.

- [Link](#)

Patchday: Adobe schließt 185 Sicherheitslücken in Experience Manager

Angreifer können Systeme mit Anwendungen von Adobe ins Visier nehmen. Nun hat der Softwarehersteller Schwachstellen geschlossen.

- [Link](#)

Patchday Microsoft: Outlook kann sich an Schadcode-E-Mail verschlucken

Microsoft hat wichtige Sicherheitsupdates für Azure, Defender & Co. veröffentlicht. Bislang soll es keine Attacken geben.

- [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-2023-5360	0.968720000	0.996320000	Link
CVE-2023-4966	0.917920000	0.986830000	Link
CVE-2023-46747	0.965530000	0.995100000	Link
CVE-2023-46604	0.968050000	0.996050000	Link
CVE-2023-42793	0.972640000	0.998190000	Link
CVE-2023-38035	0.970940000	0.997240000	Link
CVE-2023-35078	0.953010000	0.991780000	Link
CVE-2023-34634	0.900470000	0.985230000	Link
CVE-2023-34039	0.928890000	0.988160000	Link
CVE-2023-33246	0.971220000	0.997420000	Link
CVE-2023-32315	0.961510000	0.993720000	Link
CVE-2023-30625	0.941420000	0.989750000	Link
CVE-2023-30013	0.925700000	0.987810000	Link
CVE-2023-28771	0.923800000	0.987590000	Link
CVE-2023-27524	0.906990000	0.985610000	Link
CVE-2023-27372	0.971560000	0.997580000	Link
CVE-2023-27350	0.972290000	0.997990000	Link
CVE-2023-26469	0.933320000	0.988700000	Link
CVE-2023-26360	0.934340000	0.988830000	Link
CVE-2023-25717	0.962820000	0.994090000	Link
CVE-2023-25194	0.908370000	0.985750000	Link
CVE-2023-2479	0.958820000	0.993110000	Link
CVE-2023-24489	0.967670000	0.995930000	Link
CVE-2023-22518	0.967630000	0.995920000	Link
CVE-2023-22515	0.955290000	0.992300000	Link
CVE-2023-21839	0.960570000	0.993480000	Link
CVE-2023-21823	0.955130000	0.992240000	Link
CVE-2023-21554	0.961220000	0.993620000	Link
CVE-2023-20887	0.957180000	0.992700000	Link
CVE-2023-1671	0.952600000	0.991690000	Link
CVE-2023-0669	0.966690000	0.995500000	Link

BSI - Warn- und Informationsdienst (WID)

Thu, 28 Dec 2023

[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicher-

heitsvorkehrungen

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in verschiedenen SMTP Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Thu, 28 Dec 2023

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymen oder lokaler Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- [Link](#)

Thu, 28 Dec 2023

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- [Link](#)

Thu, 28 Dec 2023

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Daten zu manipulieren und seine Privilegien zu erweitern.

- [Link](#)

Thu, 28 Dec 2023

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

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

- [Link](#)

Thu, 28 Dec 2023

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Thu, 28 Dec 2023

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

Ein entfernter, authentisierter oder anonymen 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](#)

Wed, 27 Dec 2023

[NEU] [kritisch] Barracuda Networks Email Security Gateway: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Barracuda Networks Email Security Gateway ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Wed, 27 Dec 2023

[NEU] [hoch] Cacti: Mehrere Schwachstellen

Ein entfernter, anonymen oder authentifizierter Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um vertrauliche Informationen offenzulegen, Dateien zu manipulieren und beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder XSS-Angriffe durchzuführen.

- [Link](#)

Wed, 27 Dec 2023

[NEU] [hoch] ILIAS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in ILIAS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] ffmpeg: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in ffmpeg ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] PostgreSQL JDBC Treiber: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle im PostgreSQL JDBC Treiber ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Wed, 27 Dec 2023

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

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

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat Enterprise Linux (flatpak): Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in flatpak ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Wed, 27 Dec 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](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode auszuführen, ein Cross-Site-Scripting-Angriff durchzuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat Enterprise Linux Ceph Storage: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux Ceph Storage ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat Integration Camel for Spring Boot: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Integration Camel for Spring Boot ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.

- [Link](#)

Wed, 27 Dec 2023

[UPDATE] [hoch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/28/2023	[Microsoft Windows 10 1507 SEoL]	critical
12/27/2023	[NewStart CGSL MAIN 6.02 : openssl Multiple Vulnerabilities (NS-SA-2023-0074)]	critical
12/27/2023	[NewStart CGSL MAIN 5.04 : gettext Vulnerability (NS-SA-2023-0068)]	critical
12/27/2023	[NewStart CGSL MAIN 6.06 : gnutls Multiple Vulnerabilities (NS-SA-2023-0100)]	critical
12/27/2023	[GLSA-202312-16 : libssh: Multiple Vulnerabilities]	critical
12/27/2023	[GLSA-202312-17 : OpenSSH: Multiple Vulnerabilities]	critical
12/28/2023	[SUSE SLED12 / SLES12 Security Update : webkit2gtk3 (SUSE-SU-2023:4978-1)]	high
12/28/2023	[SUSE SLES15 Security Update : gstreamer (SUSE-SU-2023:4980-1)]	high
12/28/2023	[Plantronics Hub < 3.25.1 Privilege Escalation]	high
12/28/2023	[Fedora 39 : squid (2023-ab77331a34)]	high
12/28/2023	[Fedora 38 : squid (2023-6317eaa767)]	high
12/28/2023	[Moxa (CVE-2023-5961)]	high
12/27/2023	[NewStart CGSL MAIN 6.02 : expat Vulnerability (NS-SA-2023-0072)]	high
12/27/2023	[NewStart CGSL MAIN 6.02 : curl Multiple Vulnerabilities (NS-SA-2023-0071)]	high
12/27/2023	[NewStart CGSL MAIN 5.04 : expat Vulnerability (NS-SA-2023-0070)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : dnsmasq Multiple Vulnerabilities (NS-SA-2023-0078)]	high
12/27/2023	[NewStart CGSL MAIN 6.02 : binutils Multiple Vulnerabilities (NS-SA-2023-0104)]	high
12/27/2023	[NewStart CGSL MAIN 5.04 : openssl Vulnerability (NS-SA-2023-0101)]	high
12/27/2023	[NewStart CGSL MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2023-0108)]	high
12/27/2023	[NewStart CGSL MAIN 5.04 : krb5 Multiple Vulnerabilities (NS-SA-2023-0102)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : aide Vulnerability (NS-SA-2023-0093)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : python-lxml Vulnerability (NS-SA-2023-0098)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : cyrus-sasl Multiple Vulnerabilities (NS-SA-2023-0087)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : krb5 Multiple Vulnerabilities (NS-SA-2023-0096)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : dhcp Vulnerability (NS-SA-2023-0091)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : cpio Vulnerability (NS-SA-2023-0088)]	high
12/27/2023	[NewStart CGSL MAIN 6.02 : kernel Multiple Vulnerabilities (NS-SA-2023-0107)]	high

Datum	Schwachstelle	Bewertung
12/27/2023	[NewStart CGSL MAIN 6.02 : kernel Multiple Vulnerabilities (NS-SA-2023-0105)]	high
12/27/2023	[NewStart CGSL MAIN 5.04 : gzip Vulnerability (NS-SA-2023-0103)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Thu, 28 Dec 2023

Microsoft Windows PowerShell Code Execution / Event Log Bypass

Prior work from this researcher disclosed how PowerShell executes unintended files or BASE64 code when processing specially crafted filenames. This research builds on their PSTrojanFile work, adding a PS command line single quote bypass and PS event logging failure. On Windows CL tab, completing a filename uses double quotes that can be leveraged to trigger arbitrary code execution. However, if the filename got wrapped in single quotes it failed, that is until now.

- [Link](#)

” “Thu, 28 Dec 2023

Lot Reservation Management System 1.0 Shell Upload

Lot Reservation Management System version 1.0 suffers from a remote shell upload vulnerability.

- [Link](#)

” “Thu, 28 Dec 2023

Lot Reservation Management System 1.0 File Disclosure

Lot Reservation Management System version 1.0 suffers from a file disclosure vulnerability.

- [Link](#)

” “Wed, 27 Dec 2023

WhatACart 2.0.7 Cross Site Scripting

WhatACart version 2.0.7 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Tue, 26 Dec 2023

ShopSite 14.0 Cross Site Scripting

ShopSite version 14.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

” “Tue, 26 Dec 2023

FreeSWITCH 1.10.10 Denial Of Service

When handling DTLS-SRTP for media setup, FreeSWITCH version 1.10.10 is susceptible to denial of service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack.

- [Link](#)

” “Fri, 22 Dec 2023

Craft CMS 4.4.14 Remote Code Execution

This Metasploit module exploits an unauthenticated remote code execution vulnerability in Craft CMS versions 4.0.0-RC1 through 4.4.14.

- [Link](#)

” “Fri, 22 Dec 2023

Hospital Management System 4.0 XSS / Shell Upload / SQL Injection

Hospital Management System versions 4.0 and below suffer from cross site scripting, remote shell upload, and remote SQL injection vulnerabilities.

- [Link](#)

” “Fri, 22 Dec 2023

GilaCMS 1.15.4 SQL Injection

GilaCMS versions 1.15.4 and below suffer from multiple remote SQL injection vulnerabilities.

- [Link](#)

” “Thu, 21 Dec 2023

Vinchin Backup And Recovery Command Injection

This Metasploit module exploits a command injection vulnerability in Vinchin Backup & Recovery v5.0., v6.0., v6.7., and v7.0.. Due to insufficient input validation in the checkIpExists API endpoint, an attacker can execute

arbitrary commands as the web server user.

- [Link](#)

” “Thu, 21 Dec 2023

Glibc Tunables Privilege Escalation

A buffer overflow exists in the GNU C Library’s dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. It has been dubbed Looney Tunables. This issue allows an local attacker to use maliciously crafted GLIBC_TUNABLES when launching binaries with SUID permission to execute code in the context of the root user. This Metasploit module targets glibc packaged on Ubuntu and Debian. Fedora 37 and 38 and other distributions of linux also come packaged with versions of glibc vulnerable to CVE-2023-4911 however this module does not target them.

- [Link](#)

” “Wed, 20 Dec 2023

MOKOSmart MKGW1 Gateway Improper Session Management

MOKOSmart MKGW1 Gateway devices with firmware version 1.1.1 or below do not provide an adequate session management for the administrative web interface. This allows adjacent attackers with access to the management network to read and modify the configuration of the device.

- [Link](#)

” “Wed, 20 Dec 2023

TYPO3 11.5.24 Path Traversal

TYPO3 version 11.5.24 suffers from a path traversal vulnerability.

- [Link](#)

” “Wed, 20 Dec 2023

MajorDoMo Remote Code Execution

MajorDoMo versions prior to 0662e5e suffer from an unauthenticated remote code execution vulnerability.

- [Link](#)

” “Wed, 20 Dec 2023

Terrapin SSH Connection Weakening

In this paper, the authors show that as new encryption algorithms and mitigations were added to SSH, the SSH Binary Packet Protocol is no longer a secure channel: SSH channel integrity (INT-PST) is broken for three widely used encryption modes. This allows prefix truncation attacks where some encrypted packets at the beginning of the SSH channel can be deleted without the client or server noticing it. They demonstrate several real-world applications of this attack. They show that they can fully break SSH extension negotiation (RFC 8308), such that an attacker can downgrade the public key algorithms for user authentication or turn off a new countermeasure against keystroke timing attacks introduced in OpenSSH 9.5. They also identified an implementation flaw in AsyncSSH that, together with prefix truncation, allows an attacker to redirect the victim’s login into a shell controlled by the attacker. Related proof of concept code from their github has been added to this archive.

- [Link](#)

” “Tue, 19 Dec 2023

Atlassian Confluence Improper Authorization / Code Execution

This improper authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to the Confluence instance administrator. This Metasploit module uses the administrator account to install a malicious .jsp servlet plugin which the user can trigger to gain code execution on the target in the context of the of the user running the confluence server.

- [Link](#)

” “Fri, 15 Dec 2023

RTPEngine mr11.5.1.6 Denial Of Service

RTPEngine version mr11.5.1.6 suffers from a denial of service vulnerability via DTLS Hello packets during call initiation.

- [Link](#)

” “Fri, 15 Dec 2023

PKP-WAL 3.4.0-3 Remote Code Execution

PKP Web Application Library (PKP-WAL) versions 3.4.0-3 and below, as used in Open Journal Systems (OJS), Open Monograph Press (OMP), and Open Preprint Systems (OPS) before versions 3.4.0-4 or 3.3.0-16, suffer from a NativeImportExportPlugin related remote code execution vulnerability.

- [Link](#)

” “Fri, 15 Dec 2023

Asterisk 20.1.0 Denial Of Service

When handling DTLS-SRTP for media setup, Asterisk version 20.1.0 is susceptible to denial of service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack.

- [Link](#)

” “Fri, 15 Dec 2023

osCommerce 4.13-60075 Shell Upload

osCommerce version 4.13-60075 suffers from a remote shell upload vulnerability.

- [Link](#)

” “Thu, 14 Dec 2023

Chrome V8 Sandbox Escape

Proof of concept exploit for a new technique to escape from the Chrome V8 sandbox.

- [Link](#)

” “Thu, 14 Dec 2023

Chrome V8 Type Confusion / New Sandbox Escape

Proof of concept exploit for CVE-2023-3079 that leverages a type confusion in V8 in Google Chrome versions prior to 114.0.5735.110. This issue allows a remote attacker to potentially exploit heap corruption via a crafted HTML page. This variant of the exploit applies a new technique to escape the sandbox.

- [Link](#)

” “Thu, 14 Dec 2023

Chrome V8 JIT XOR Arbitrary Code Execution

Chrome V8 proof of concept exploit for CVE-2021-21220. The specific flaw exists within the implementation of XOR operation when executed within JIT compiled code.

- [Link](#)

” “Thu, 14 Dec 2023

Chrome V8 Type Confusion

Proof of concept exploit for CVE-2023-3079 that leverages a type confusion in V8 in Google Chrome versions prior to 114.0.5735.110. This issue allows a remote attacker to potentially exploit heap corruption via a crafted HTML page.

- [Link](#)

” “Thu, 14 Dec 2023

Windows Kernel Race Conditions

The Microsoft Windows Kernel has an issue with bad locking in registry virtualization that can result in race conditions.

- [Link](#)

”

0-Days der letzten 5 Tage

Die Hacks der Woche

mit Martin Haunschmid

Ihr habt WAS in eure Züge programmiert!?



[Zum Youtube Video](#)

Cyberangriffe: (Dez)

Datum	Opfer	Land	Information
2023-12-27	Eagers Automotive	[AUS]	Link
2023-12-26	National Insurance Board of Trinidad and Tobago (NIBTT)	[TTO]	Link
2023-12-26	Syndicat Général des Vignerons de la Champagne	[FRA]	Link
2023-12-24	Katholische Hospitalvereinigung Ostwestfalen (KHO)	[DEU]	Link
2023-12-24	Cullman County Courthouse	[USA]	Link
2023-12-23	Commune de Härjedalen	[SWE]	Link
2023-12-21	Le département de l'Urbanisme et du Logement de Madhya Pradesh (Inde).	[IND]	Link
2023-12-21	Universität Innsbruck	[AUT]	Link
2023-12-21	Ohio Lottery	[USA]	Link
2023-12-20	Kitco	[CAN]	Link
2023-12-20	First American	[USA]	Link
2023-12-20	Ubisoft	[FRA]	Link
2023-12-19	HCL Technologies	[IND]	Link
2023-12-19	St Vincent's Health Australia	[AUS]	Link
2023-12-19	Liberty Hospital.	[USA]	Link
2023-12-18	Elektroprivreda Srbije (EPS)	[SRB]	Link
2023-12-17	Socadis	[CAN]	Link
2023-12-16	Confédération Luxembourgeoise des Syndicats (LCGB)	[LUX]	Link
2023-12-15	Yakult Australia	[AUS]	Link
2023-12-14	Verocard	[BRA]	Link
2023-12-13	Limburg.net	[BEL]	Link
2023-12-13	London Public Library	[CAN]	Link
2023-12-13	Agência Nacional de Águas e Saneamento Básico (ANA)	[BRA]	Link
2023-12-13	VF Corp	[USA]	Link
2023-12-13	MongoDB	[USA]	Link
2023-12-13	Western Railway's Lower Parel workshop	[IND]	Link
2023-12-12	District de March	[CHE]	Link
2023-12-12	Hotelplan UK	[GBR]	Link
2023-12-11	Banque centrale du Lesotho	[LSO]	Link
2023-12-11	Milton Town School District (MTSD)	[USA]	Link
2023-12-10	Jysk Energi	[DNK]	Link
2023-12-10	EasyPark	[NLD]	Link
2023-12-10	CACG (Compagnie d'Aménagement des Coteaux de Gascogne)	[FRA]	Link
2023-12-09	Mairie d'Ozoir-la-Ferrière	[FRA]	Link
2023-12-08	Province des îles Loyauté	[NCL]	Link
2023-12-08	WestPole	[ITA]	Link
2023-12-08	Coaxis	[FRA]	Link
2023-12-08	Kaunas University of Technology (KTU)	[LTU]	Link
2023-12-07	Aqualectra	[CUW]	Link
2023-12-07	Université de Wollongong	[AUS]	Link
2023-12-07	Prefeitura de Poços de Caldas	[BRA]	Link
2023-12-07	Hinsdale School District	[USA]	Link
2023-12-06	Nissan Oceania	[AUS]	Link
2023-12-06	Gouvernement du Yucatan	[MEX]	Link
2023-12-06	Université de Sherbrooke	[CAN]	Link
2023-12-06	Glendale Unified School District	[USA]	Link
2023-12-06	Groveport Madison School District	[USA]	Link
2023-12-05	Dameron Hospital	[USA]	Link
2023-12-05	Gräbener Maschinentechnik	[DEU]	Link
2023-12-04	Caribbean Community (Caricom) Secretariat	[GUY]	Link
2023-12-01	Communauté de communes du Pays du Neubourg	[FRA]	Link

Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-28	[americanalarm.com]	blackbasta	Link
2023-12-28	[gdi.com]	cactus	Link
2023-12-28	[bachoco.com.mx]	cactus	Link
2023-12-28	[pbssystem.com]	cactus	Link
2023-12-28	[Northland Mechanical Contractors]	bianlian	Link
2023-12-28	[Wesgar Inc]	alphv	Link
2023-12-28	[CVR Associates]	play	Link
2023-12-25	[hoffmanestates.org]	lockbit3	Link
2023-12-25	[coastalplainsctr.org]	lockbit3	Link
2023-12-27	[webblaw.com]	blackbasta	Link
2023-12-27	[Ohio Lottery]	dragonforce	Link
2023-12-27	[EPS.RS]	qilin	Link
2023-12-27	[Lake of the Woods County]	meow	Link
2023-12-27	[Ultra Intelligence & Communications]	alphv	Link
2023-12-27	[Aura Engineering, LLC]	alphv	Link
2023-12-27	[FIRST 5 Santa Clara County]	alphv	Link
2023-12-27	[ecom.gov.il]	toufan	Link
2023-12-27	[maytronics.com]	toufan	Link
2023-12-26	[richmont.edu]	lockbit3	Link
2023-12-26	[coaxis.com]	lockbit3	Link
2023-12-26	[smbw.com.au]	lockbit3	Link
2023-12-26	[Regarding FM]	raznatovic	Link
2023-12-26	[carolinalemke.com]	toufan	Link
2023-12-26	[ari.co.il]	toufan	Link
2023-12-26	[Abdali Hospital]	rhysida	Link
2023-12-26	[Tshwane University of Technology]	rhysida	Link
2023-12-25	[Blaine County Schools]	blacksuit	Link
2023-12-25	[pcmarket.uz]	stormous	Link
2023-12-25	[International Electronic Machines Corp]	akira	Link
2023-12-25	[co.pickens.sc.us]	lockbit3	Link
2023-12-25	[walkro.eu]	lockbit3	Link
2023-12-25	[ontariopork.on.ca]	lockbit3	Link
2023-12-25	[zrvp.ro]	lockbit3	Link
2023-12-25	[tecnifibre.com]	lockbit3	Link
2023-12-25	[hendelsinc.com]	lockbit3	Link
2023-12-20	[Horizon Pool and Spa]	8base	Link
2023-12-20	[Davis Cedillo and Mendoza Inc]	8base	Link
2023-12-24	[Ono Academic College]	malekteam	Link
2023-12-24	[dorimedia]	malekteam	Link
2023-12-24	[gav.co.il]	malekteam	Link
2023-12-24	[ZIV Hospital]	malekteam	Link
2023-12-24	[Prefeitura Municipal de Itabira]	alphv	Link
2023-12-24	[bkf-fleuren.de]	lockbit3	Link
2023-12-23	[avescorent.ch]	lockbit3	Link
2023-12-23	[allot.com]	toufan	Link
2023-12-23	[Bay Orthopedic & Rehabilitation Supply]	bianlian	Link
2023-12-15	[forabank.ru]	werewolves	Link
2023-12-17	[vasexperts.ru]	werewolves	Link
2023-12-23	[zurcherodioraven.com]	lockbit3	Link
2023-12-23	[quakerwindows.com]	cactus	Link
2023-12-23	[bconnect.co.il]	toufan	Link
2023-12-23	[super-pharm.co.il]	toufan	Link
2023-12-23	[PriceSmart (Update)]	alphv	Link
2023-12-23	[castores.com.mx]	lockbit3	Link
2023-12-22	[VF Corporation]	alphv	Link
2023-12-22	[ciasc.mx]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-22	[csmsa.com.ar]	lockbit3	Link
2023-12-22	[whafh.com]	blackbasta	Link
2023-12-22	[hotelplan.co.uk]	blackbasta	Link
2023-12-22	[Nissan Australia]	akira	Link
2023-12-22	[xeinadin.com]	lockbit3	Link
2023-12-22	[igs-inc.com]	lockbit3	Link
2023-12-22	[teldor.com]	toufan	Link
2023-12-22	[erco.co.il]	toufan	Link
2023-12-22	[esepac.com]	lockbit3	Link
2023-12-22	[fager-mcgee.com]	lockbit3	Link
2023-12-22	[goldenc.com]	lockbit3	Link
2023-12-22	[sterlinghomes.com.au]	lockbit3	Link
2023-12-22	[denford.co.uk]	lockbit3	Link
2023-12-21	[comtrade.com]	stormous	Link
2023-12-21	[zewailcity.edu.eg]	stormous	Link
2023-12-21	[evn.com.vn]	stormous	Link
2023-12-21	[inwi.ma]	stormous	Link
2023-12-21	[rmutto.ac.th]	stormous	Link
2023-12-21	[trabzon.edu.tr]	stormous	Link
2023-12-21	[ACE Air Cargo]	dragonforce	Link
2023-12-21	[Kinetic Leasing]	dragonforce	Link
2023-12-13	[dillarddoor.com]	cactus	Link
2023-12-16	[cts.co.uk]	cactus	Link
2023-12-20	[hunterbuildings.com]	cactus	Link
2023-12-20	[larlyn.com]	cactus	Link
2023-12-20	[wkw-group.com]	cactus	Link
2023-12-20	[dbmgroupp.com]	cactus	Link
2023-12-20	[Jon Richard]	play	Link
2023-12-20	[Concept Data]	play	Link
2023-12-20	[Packaging Solutions]	play	Link
2023-12-21	[Owen Quilty Professional]	play	Link
2023-12-21	[zonesoft.pt]	stormous	Link
2023-12-21	[zonesoft.pt]	ranstreet	Link
2023-12-20	[Yakult Australia]	dragonforce	Link
2023-12-20	[Bladen County Public Library]	meow	Link
2023-12-20	[smudlers.com]	lockbit3	Link
2023-12-20	[Unite Here]	incransom	Link
2023-12-20	[tefentech.com]	toufan	Link
2023-12-20	[zoko.co.il]	toufan	Link
2023-12-20	[Di Martino Group]	ragroup	Link
2023-12-20	[Rockford Gastroenterology Associates]	ragroup	Link
2023-12-20	[HALLIDAYS GROUP LIMITED]	ragroup	Link
2023-12-20	[Die Unfallkasse Thüringen]	ragroup	Link
2023-12-20	[NIDEC GPM GmbH]	ragroup	Link
2023-12-20	[dobsystems.com]	lockbit3	Link
2023-12-20	[des-igngroup.com]	lockbit3	Link
2023-12-20	[Navigation Financial Group]	alphv	Link
2023-12-20	[udhaiyamdhall.com]	lockbit3	Link
2023-12-20	[Air Sino-Euro Associates Travel Pte. Ltd]	bianlian	Link
2023-12-20	[LCGB]	8base	Link
2023-12-20	[CETEC Ingénierie]	8base	Link
2023-12-20	[The International School of Management]	8base	Link
2023-12-20	[Employ Milwaukee]	8base	Link
2023-12-20	[Horizon Pool & Spa]	8base	Link
2023-12-20	[socadis]	8base	Link
2023-12-20	[Davis Cedillo & Mendoza Inc]	8base	Link
2023-12-20	[spiritleatherworks.com]	lockbit3	Link
2023-12-19	[strauss-group.com]	toufan	Link
2023-12-19	[RCSB PDB]	meow	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-19	[mtsd-vt.org]	lockbit3	Link
2023-12-19	[Viking Therapeutics]	alphv	Link
2023-12-19	[www.pts-tools.com]	toufan	Link
2023-12-19	[www.plasson-pead.com.br]	toufan	Link
2023-12-19	[www.nistx.com]	toufan	Link
2023-12-19	[www.ktstooling.com]	toufan	Link
2023-12-19	[www.herrickindustrial.com]	toufan	Link
2023-12-19	[www.drillmex.com]	toufan	Link
2023-12-19	[www.dixie-tool.com]	toufan	Link
2023-12-19	[www.copreinternacional.com]	toufan	Link
2023-12-19	[www.butlerbros.com]	toufan	Link
2023-12-19	[www.atwoodindustries.com]	toufan	Link
2023-12-19	[wsies.com]	toufan	Link
2023-12-19	[vehicle.touch-ins.co.il]	toufan	Link
2023-12-19	[tryhardindustrial.ca]	toufan	Link
2023-12-19	[sys.udidagan.co.il]	toufan	Link
2023-12-19	[sys.touch-ins.co.il]	toufan	Link
2023-12-19	[sys-cspartnershq1.caesarstone.com]	toufan	Link
2023-12-19	[sys-cspartners.caesarstoneus.com]	toufan	Link
2023-12-19	[sys-cspartners.caesarstone.sg]	toufan	Link
2023-12-19	[sys-cspartners.caesarstone.co.uk]	toufan	Link
2023-12-19	[sys-cspartners.caesarstone.com.au]	toufan	Link
2023-12-19	[sys-cspartners.caesarstone.ca]	toufan	Link
2023-12-19	[sys.biopet.co.il]	toufan	Link
2023-12-19	[store.toolneeds.com]	toufan	Link
2023-12-19	[store.brunswickindustrial.com]	toufan	Link
2023-12-19	[stage.kravitz.co.il]	toufan	Link
2023-12-19	[shop.smithindustrialsupply.com]	toufan	Link
2023-12-19	[shop.shopsupply.net]	toufan	Link
2023-12-19	[shop.reggiemckenzieindustrial.com]	toufan	Link
2023-12-19	[shop.qct.tools]	toufan	Link
2023-12-19	[shop.lgindustrial.com]	toufan	Link
2023-12-19	[shop.emprecise.com]	toufan	Link
2023-12-19	[shop.clador.com]	toufan	Link
2023-12-19	[shop.britecon.com]	toufan	Link
2023-12-19	[shefa-online.co.il]	toufan	Link
2023-12-19	[selwayindustrialsupply.com]	toufan	Link
2023-12-19	[rocket-supply.com]	toufan	Link
2023-12-19	[rmpis.com]	toufan	Link
2023-12-19	[reserved-il.com]	toufan	Link
2023-12-19	[pts-tools.com]	toufan	Link
2023-12-19	[product.touch-ins.co.il]	toufan	Link
2023-12-19	[pmt-usa.com]	toufan	Link
2023-12-19	[phoenix.touch-ins.co.il]	toufan	Link
2023-12-19	[pet.touch-ins.co.il]	toufan	Link
2023-12-19	[pet.biopet.co.il]	toufan	Link
2023-12-19	[paragon-supply.com]	toufan	Link
2023-12-19	[old.shefa-online.co.il]	toufan	Link
2023-12-19	[norviktools.com]	toufan	Link
2023-12-19	[northernprecisionsales.com]	toufan	Link
2023-12-19	[newstore.johnstoncompanies.com]	toufan	Link
2023-12-19	[mortgage.touch-ins.co.il]	toufan	Link
2023-12-19	[morsecuttingtools.com]	toufan	Link
2023-12-19	[mitchellmckinney.com]	toufan	Link
2023-12-19	[mgisales.com]	toufan	Link
2023-12-19	[m.biopet.co.il]	toufan	Link
2023-12-19	[libertytool.com]	toufan	Link
2023-12-19	[ktstooling.com]	toufan	Link
2023-12-19	[knightesupply.com]	toufan	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-19	[keter.com]	toufan	Link
2023-12-19	[keter.co.il]	toufan	Link
2023-12-19	[its-supply.com]	toufan	Link
2023-12-19	[h-o.co.il]	toufan	Link
2023-12-19	[goronco.com]	toufan	Link
2023-12-19	[gordonindustrial.com]	toufan	Link
2023-12-19	[global.keter.com]	toufan	Link
2023-12-19	[giddirect.com]	toufan	Link
2023-12-19	[gfwdsupply.com]	toufan	Link
2023-12-19	[fugatesales.com]	toufan	Link
2023-12-19	[drillmex.com]	toufan	Link
2023-12-19	[dixie-tool.com]	toufan	Link
2023-12-19	[detsupply.com]	toufan	Link
2023-12-19	[cspartnershq1.caesarstone.com]	toufan	Link
2023-12-19	[cspartners.caesarstoneus.com]	toufan	Link
2023-12-19	[cspartners.caesarstone.sg]	toufan	Link
2023-12-19	[cspartners.caesarstone.co.uk]	toufan	Link
2023-12-19	[cspartners.caesarstone.com.au]	toufan	Link
2023-12-19	[cspartners.caesarstone.ca]	toufan	Link
2023-12-19	[core.touch-ins.co.il]	toufan	Link
2023-12-19	[copreinternacional.com]	toufan	Link
2023-12-19	[colmarindustrial.com]	toufan	Link
2023-12-19	[cmtindustrial.com]	toufan	Link
2023-12-19	[cdt1.com]	toufan	Link
2023-12-19	[catalog.ustg.net]	toufan	Link
2023-12-19	[catalog.toolkrib.com]	toufan	Link
2023-12-19	[catalog.fotcnc.com]	toufan	Link
2023-12-19	[cartersoshkosh.co.il]	toufan	Link
2023-12-19	[butlerbros.com]	toufan	Link
2023-12-19	[blueashsupply.com]	toufan	Link
2023-12-19	[berkshireesupply.com]	toufan	Link
2023-12-19	[barindustrial.com]	toufan	Link
2023-12-19	[badgermill.com]	toufan	Link
2023-12-19	[atwoodindustries.com]	toufan	Link
2023-12-19	[arieladar.com]	toufan	Link
2023-12-19	[api.touch-ins.co.il]	toufan	Link
2023-12-19	[apisinc.com]	toufan	Link
2023-12-19	[amtektool.com]	toufan	Link
2023-12-19	[allegHENYtool.net]	toufan	Link
2023-12-19	[alcornindustrial.com]	toufan	Link
2023-12-19	[ustg.net]	toufan	Link
2023-12-19	[chuzefitness.com]	lockbit3	Link
2023-12-19	[brintons.co.uk]	blackbasta	Link
2023-12-19	[pecofoods.com]	blackbasta	Link
2023-12-19	[Kauno Technologijos Universitetas]	rhysida	Link
2023-12-18	[Blackstone Valley Community Health Care]	hunters	Link
2023-12-18	[Richard Harris Personal Injury Law Firm]	play	Link
2023-12-18	[Schoepe Display]	play	Link
2023-12-18	[Waldner's]	play	Link
2023-12-18	[Succes Schoonmaak]	play	Link
2023-12-18	[DYWIDAG-Systems & American Transportation]	play	Link
2023-12-18	[C????z????]	play	Link
2023-12-18	[The CM Paula]	play	Link
2023-12-18	[parat-technology.com]	lockbit3	Link
2023-12-18	[Viking Therapeutics reported to the SEC following a breach]	alphv	Link
2023-12-18	[naandanjain.com]	toufan	Link
2023-12-18	[LAJOLLAGROUP]	cactus	Link
2023-12-18	[Ta-Supply.com]	toufan	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-18	[Electrical Connections]	bianlian	Link
2023-12-18	[navitaspet.com]	blackbasta	Link
2023-12-18	[vyera.com]	blackbasta	Link
2023-12-18	[hallidays.co.uk]	blackbasta	Link
2023-12-17	[techno-rezef.com]	toufan	Link
2023-12-17	[curver.com]	toufan	Link
2023-12-17	[dorot.com]	toufan	Link
2023-12-17	[graf.co.il]	toufan	Link
2023-12-17	[brother.co.il]	toufan	Link
2023-12-17	[ATCO Products Inc]	medusa	Link
2023-12-17	[Biomatrix LLC]	medusa	Link
2023-12-17	[TechKids aka MindX]	raznatovic	Link
2023-12-17	[SKF.com]	raznatovic	Link
2023-12-17	[Colonial Pipeline]	raznatovic	Link
2023-12-17	[rodo.co.uk]	lockbit3	Link
2023-12-16	[E & J Gallo Winery]	alphv	Link
2023-12-14	[Kraft Foods]	snatch	Link
2023-12-14	[Spaulding Clinical]	snatch	Link
2023-12-16	[Crace Medical Centre]	knight	Link
2023-12-16	[DSG-US.COM]	cl0p	Link
2023-12-16	[New York School of Interior Design]	incransom	Link
2023-12-16	[CTS]	cactus	Link
2023-12-16	[kohlwholesale.com]	blackbasta	Link
2023-12-16	[Insidesource]	8base	Link
2023-12-15	[hebel.com]	lockbit3	Link
2023-12-15	[Nexiga]	akira	Link
2023-12-07	[CIE]	cactus	Link
2023-12-07	[NNDOMAIN]	cactus	Link
2023-12-11	[ISC]	cactus	Link
2023-12-13	[DILLARD]	cactus	Link
2023-12-15	[Fred Hutchinson Cancer Research Center]	hunters	Link
2023-12-14	[bemes.com]	lockbit3	Link
2023-12-14	[mcs360.com]	lockbit3	Link
2023-12-14	[goldwind.com]	lockbit3	Link
2023-12-14	[converzmedia.com]	lockbit3	Link
2023-12-14	[rpassoc.com]	lockbit3	Link
2023-12-14	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry]	bianlian	Link
2023-12-14	[Commonwealth Capital]	bianlian	Link
2023-12-14	[Greenbox Loans Inc.]	bianlian	Link
2023-12-14	[Hyman Hayes Associates]	akira	Link
2023-12-14	[grandrapidswomenshealth.com]	lockbit3	Link
2023-12-14	[pcli.com]	lockbit3	Link
2023-12-13	[austen-it.com]	lockbit3	Link
2023-12-08	[Akir Metal San Tic Ltd ti was hacked. All confidential information was stolen]	knight	Link
2023-12-13	[Gaido-fintzen.com]	cloak	Link
2023-12-13	[DAIHO INDUSTRIAL Co.,Ltd.]	knight	Link
2023-12-13	[cityofdefiance.com]	knight	Link
2023-12-13	[Heart of Texas Region MHMR]	dragonforce	Link
2023-12-13	[PCTEL]	dragonforce	Link
2023-12-13	[Agl Welding Supply]	dragonforce	Link
2023-12-13	[Grayhill]	dragonforce	Link
2023-12-13	[Leederson Lighting]	dragonforce	Link
2023-12-13	[Coca-Cola Singapore]	dragonforce	Link
2023-12-13	[Shorts]	dragonforce	Link
2023-12-13	[World Emblem International]	dragonforce	Link
2023-12-13	[The GBUAHN]	dragonforce	Link
2023-12-13	[Baden]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-13	[Dafiti Argentina]	dragonforce	Link
2023-12-13	[Lunacon Construction Group]	dragonforce	Link
2023-12-13	[Tglt]	dragonforce	Link
2023-12-13	[Seven Seas]	dragonforce	Link
2023-12-13	[Decina]	dragonforce	Link
2023-12-13	[Cooper Research Technology]	dragonforce	Link
2023-12-13	[Greater Cincinnati Behavioral Health]	dragonforce	Link
2023-12-13	[ccadm.org]	lockbit3	Link
2023-12-13	[dawsongroup.co.uk]	lockbit3	Link
2023-12-13	[altezze.com.mx]	lockbit3	Link
2023-12-13	[Tulane University]	meow	Link
2023-12-13	[thirdstreetbrewhouse.com carolinabeveragegroup.com]	blackbasta	Link
2023-12-13	[Advantage Group International]	alphv	Link
2023-12-13	[Dameron Hospital]	ransomhouse	Link
2023-12-13	[agy.com]	blackbasta	Link
2023-12-13	[alexander-dennis.com]	blackbasta	Link
2023-12-13	[Dillard Door & Security]	cactus	Link
2023-12-13	[cms.law]	lockbit3	Link
2023-12-13	[SBK Real Estate]	8base	Link
2023-12-13	[CACG]	8base	Link
2023-12-13	[VAC-U-MAX]	8base	Link
2023-12-13	[Hawkins Sales]	8base	Link
2023-12-13	[William Jackson Food Group]	8base	Link
2023-12-13	[Groupe PROMOBÉ]	8base	Link
2023-12-13	[Soethoudt metaalbewerking b.v.]	8base	Link
2023-12-13	[REUS MOBILITAT I SERVEIS]	8base	Link
2023-12-13	[Tim Davies Landscaping]	8base	Link
2023-12-12	[King Aerospace, Inc.]	incransom	Link
2023-12-12	[GlobalSpec]	play	Link
2023-12-12	[dena.de]	lockbit3	Link
2023-12-12	[woodruffenterprises.com]	threeam	Link
2023-12-12	[shareharris.com]	threeam	Link
2023-12-12	[SmartWave Technologies]	akira	Link
2023-12-12	[Mitrani Caballero Ojam & Ruiz Moreno - Abogados]	akira	Link
2023-12-12	[The Teaching Company, LLC]	akira	Link
2023-12-12	[Memorial Sloan Kettering Cancer Center]	meow	Link
2023-12-12	[petrotec.com.qa]	lockbit3	Link
2023-12-12	[tradewindscorp-insbrok.com]	lockbit3	Link
2023-12-12	[airtechthelong.com.vn]	lockbit3	Link
2023-12-12	[kitahirosima.jp]	lockbit3	Link
2023-12-12	[Grupo Jose Alves]	rhysida	Link
2023-12-12	[Insomniac Games]	rhysida	Link
2023-12-11	[phillipsglobal.us]	lockbit3	Link
2023-12-11	[greenbriersportingclub.com]	lockbit3	Link
2023-12-11	[ipp-sa.com]	lockbit3	Link
2023-12-11	[r-ab.de]	lockbit3	Link
2023-12-11	[Azienda USL di Modena]	hunters	Link
2023-12-11	[igt.nl]	lockbit3	Link
2023-12-01	[Bayer Heritage Federal Credit Union]	lorenz	Link
2023-12-11	[MSD Information technology]	akira	Link
2023-12-11	[Goiasa]	akira	Link
2023-12-11	[Hinsdale School District]	medusa	Link
2023-12-11	[Independent Recovery Resources, Inc.]	bianlian	Link
2023-12-11	[Studio MF]	akira	Link
2023-12-11	[zailaboratory.com]	lockbit3	Link
2023-12-11	[ISC Consulting Engineers]	cactus	Link
2023-12-11	[The Glendale Unified School District]	medusa	Link
2023-12-10	[pronatindustries.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-10	[policia.gob.pe]	lockbit3	Link
2023-12-10	[Holding Slovenske elektrarne]	rhysida	Link
2023-12-10	[Hse]	rhysida	Link
2023-12-09	[Qatar Racing and Equestrian Club]	rhysida	Link
2023-12-09	[Graphic Solutions Group Inc (US)]	daixin	Link
2023-12-09	[OpTransRights - 2]	siegedsec	Link
2023-12-09	[Telerad]	siegedsec	Link
2023-12-09	[Technical University of Mombasa]	siegedsec	Link
2023-12-09	[National Office for centralized procurement]	siegedsec	Link
2023-12-09	[Portland Government & United states government]	siegedsec	Link
2023-12-09	[Staples]	siegedsec	Link
2023-12-09	[Deqing County]	siegedsec	Link
2023-12-09	[Colombian National Registry]	siegedsec	Link
2023-12-09	[HMW - Press Release]	monti	Link
2023-12-08	[livanova.com]	lockbit3	Link
2023-12-04	[Jerry Pate Energy (hack from Saltmarsh Financial Advisors)]	snatch	Link
2023-12-08	[GOLFZON]	blacksuit	Link
2023-12-08	[aw-lawyers.com]	lockbit3	Link
2023-12-08	[midlandindustries.com]	lockbit3	Link
2023-12-08	[Travian Games]	rhysida	Link
2023-12-08	[Tcman]	rhysida	Link
2023-12-07	[California Innovations]	play	Link
2023-12-07	[SMRT]	play	Link
2023-12-07	[Intrepid Sea, Air & Space Museum]	play	Link
2023-12-07	[Postworks]	play	Link
2023-12-07	[PLS Logistics]	play	Link
2023-12-07	[Ridge Vineyards]	play	Link
2023-12-07	[AJO]	play	Link
2023-12-07	[PHIBRO GMBH]	play	Link
2023-12-07	[denave.com]	lockbit3	Link
2023-12-07	[Precision Technologies Group Ltd]	incransom	Link
2023-12-07	[Silvent North America]	play	Link
2023-12-07	[GreenWaste Recovery]	play	Link
2023-12-07	[Burton Wire & Cable]	play	Link
2023-12-07	[Capespan]	play	Link
2023-12-07	[Becker Furniture World]	play	Link
2023-12-07	[Payne Hicks Beach]	play	Link
2023-12-07	[Vitro Plus]	play	Link
2023-12-07	[GVM]	play	Link
2023-12-07	[Planbox]	play	Link
2023-12-07	[AG Consulting Engineering]	play	Link
2023-12-07	[Greater Richmond Transit]	play	Link
2023-12-07	[Kuriyama of America]	play	Link
2023-12-07	[bluewaterstt.com]	lockbit3	Link
2023-12-07	[omegapainclinic.com]	lockbit3	Link
2023-12-07	[AMCO Proteins]	bianlian	Link
2023-12-07	[SML Group]	bianlian	Link
2023-12-07	[stormtech]	metaencryptor	Link
2023-12-07	[Garda]	metaencryptor	Link
2023-12-07	[Tri-city Medical Center]	incransom	Link
2023-12-07	[Tasteful Selections]	akira	Link
2023-12-07	[Ware Manufacturing]	qilin	Link
2023-12-07	[Neurology Center of Nevada]	qilin	Link
2023-12-07	[CIE Automotive]	cactus	Link
2023-12-07	[National Nail Corp]	cactus	Link
2023-12-07	[citizenswv.com]	lockbit3	Link
2023-12-07	[directradiology.com]	lockbit3	Link
2023-12-07	[signiflow.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-07	[bpce.com]	lockbit3	Link
2023-12-07	[hopito.com]	lockbit3	Link
2023-12-07	[usherbrooke.ca]	lockbit3	Link
2023-12-07	[Visan]	8base	Link
2023-12-07	[Tryax Realty Management - Press Release]	monti	Link
2023-12-06	[Campbell County Schools]	medusa	Link
2023-12-06	[Deutsche Energie-Agentur]	alphv	Link
2023-12-06	[Compass Group Italia]	akira	Link
2023-12-06	[Aqualectra Holdings]	akira	Link
2023-12-06	[Acero Engineering]	bianlian	Link
2023-12-06	[syrtech.com]	threeam	Link
2023-12-06	[ACCU Reference Medical Lab]	medusa	Link
2023-12-06	[Sagent]	medusa	Link
2023-12-06	[fpz.com]	lockbit3	Link
2023-12-06	[labelians.fr]	lockbit3	Link
2023-12-06	[polyclinique-cotentin.com]	lockbit3	Link
2023-12-06	[Lischkoff and Pitts, P.C.]	8base	Link
2023-12-06	[SMG Confrere]	8base	Link
2023-12-06	[Calgary TELUS Convention Centre]	8base	Link
2023-12-06	[astley.]	8base	Link
2023-12-05	[Henry Schein Inc - Henry's " LOST SHINE "]	alphv	Link
2023-12-05	[TraCS Florida FSU]	alphv	Link
2023-12-05	[aldoshoes.com]	lockbit3	Link
2023-12-05	[laprensani.com]	lockbit3	Link
2023-12-05	[mapc.org]	lockbit3	Link
2023-12-05	[ussignandmill.com]	threeam	Link
2023-12-05	[Rudolf-Venture Chemical Inc - Part 1]	monti	Link
2023-12-05	[Akumin]	bianlian	Link
2023-12-05	[CLATSKANIEPUD]	alphv	Link
2023-12-05	[restargp.com]	lockbit3	Link
2023-12-05	[concertus.co.uk]	abyss	Link
2023-12-05	[Bowden Barlow Law PA]	medusa	Link
2023-12-05	[Rosens Diversified Inc]	medusa	Link
2023-12-05	[Henry County Schools]	blacksuit	Link
2023-12-05	[fps.com]	blacksuit	Link
2023-12-04	[Full access to the school network USA]	everest	Link
2023-12-04	[CMS Communications]	qilin	Link
2023-12-04	[Tipalti]	alphv	Link
2023-12-04	[Great Lakes Technologies]	qilin	Link
2023-12-04	[Midea Carrier]	akira	Link
2023-12-04	[ychlccsc.edu.hk]	lockbit3	Link
2023-12-04	[nlt.com]	blackbasta	Link
2023-12-04	[Getrix]	akira	Link
2023-12-04	[Evnhcmc]	alphv	Link
2023-12-03	[mirle.com.tw]	lockbit3	Link
2023-12-03	[Bern Hotels & Resorts]	akira	Link
2023-12-03	[Tipalti claimed as a victim - but we'll extort Roblox and Twitch, two of their affected cl]	alphv	Link
2023-12-03	[Tipalti claimed as a victim - but we'll extort Roblox, one of their affected clients, indi]	alphv	Link
2023-12-02	[Lisa Mayer CA, Professional Corporation]	alphv	Link
2023-12-02	[bboed.org]	lockbit3	Link
2023-12-01	[hnnscsb.org]	lockbit3	Link
2023-12-01	[elsewedyelectric.com]	lockbit3	Link
2023-12-01	[Austal USA]	hunters	Link
2023-12-02	[inseinc.com]	blackbasta	Link
2023-12-02	[royaleinternational.com]	alphv	Link
2023-12-01	[Dörr Group]	alphv	Link
2023-12-01	[IRC Engineering]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-01	[Hello Cristina from Law Offices of John E Hill]	monti	Link
2023-12-01	[Hello Jacobs from RVC]	monti	Link
2023-12-01	[Austal]	hunters	Link
2023-12-01	[St. Johns River Water Management District]	hunters	Link
2023-12-01	[Kellett & Bartholow PLLC]	incransom	Link
2023-12-01	[Centroedile Milano]	blacksuit	Link
2023-12-01	[Iptor]	akira	Link
2023-12-01	[farwickgrote.de]	cloak	Link
2023-12-01	[skncustoms.com]	cloak	Link
2023-12-01	[euro2000-spa.it]	cloak	Link
2023-12-01	[Thenewtrongroup.com]	cloak	Link
2023-12-01	[Bankofceylon.co.uk]	cloak	Link
2023-12-01	[carranza.on.ca]	cloak	Link
2023-12-01	[Agamatrix]	meow	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.