



Ausgabe: 20231226

# 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 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](#)

---

### ***Sicherheitsupdate Apache Struts: Uploadfunktion kann Schadcode passieren lassen***

Eine kritische Schwachstelle bedroht das Open-Source-Framework Apache Struts.

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

## BSI - Warn- und Informationsdienst (WID)

Fri, 22 Dec 2023

*[NEU] [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](#)

---

Fri, 22 Dec 2023

### *[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes*

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux und CentOS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen oder einen Denial of Service zu verursachen.

- [Link](#)

---

Fri, 22 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](#)

---

Fri, 22 Dec 2023

### *[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen*

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen.

- [Link](#)

---

Fri, 22 Dec 2023

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

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

- [Link](#)

---

Fri, 22 Dec 2023

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

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

- [Link](#)

---

Fri, 22 Dec 2023

### *[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen*

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

---

Fri, 22 Dec 2023

### *[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen*

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

---

Fri, 22 Dec 2023

### *[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen*

Ein Angreifer kann mehrere Schwachstellen in Splunk Enterprise ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- [Link](#)

---

Fri, 22 Dec 2023

### *[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung*

Ein Angreifer in Funk-Reichweite kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 22 Dec 2023

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

---

Fri, 22 Dec 2023

**[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen oder um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Thu, 21 Dec 2023

**[NEU] [hoch] Moodle: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, Code auszuführen, einen Denial-of-Service-Angriff zu starten, Informationen offen zu legen und Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Thu, 21 Dec 2023

**[NEU] [hoch] Ivanti Avalanche: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ivanti Avalanche ausnutzen, um Code auszuführen, einen Denial of Service zu verursachen, Informationen preiszugeben und Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Thu, 21 Dec 2023

**[UPDATE] [hoch] Squid: Schwachstelle ermöglicht Denial of Service**

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

- [Link](#)

---

Thu, 21 Dec 2023

**[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen**

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

- [Link](#)

---

Thu, 21 Dec 2023

**[UPDATE] [kritisch] D-LINK G416 Router: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen im D-LINK G416 Routern ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

---

Thu, 21 Dec 2023

**[UPDATE] [hoch] Squid: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Thu, 21 Dec 2023

**[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen**

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

- [Link](#)

---

Thu, 21 Dec 2023

**[UPDATE] [hoch] Squid: Schwachstelle ermöglicht Denial of Service**

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

- [Link](#)

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/23/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : zbar (SUSE-SU-2023:4948-1)]	critical
12/23/2023	[GLSA-202312-11 : SABnzbd: Remote Code Execution]	critical
12/22/2023	[CentOS 7 : firefox (RHSA-2023:3579)]	critical
12/22/2023	[CentOS 7 : firefox (RHSA-2023:5477)]	critical
12/22/2023	[CentOS 7 : firefox (RHSA-2023:6162)]	critical
12/22/2023	[Nutanix AHV : Multiple Vulnerabilities (NXSA-AHV-20230302.1011)]	critical
12/22/2023	[Oracle Linux 9 : kernel (ELSA-2023-7749)]	critical
12/25/2023	[openSUSE 15 Security Update : cppcheck (openSUSE-SU-2023:0413-1)]	high
12/24/2023	[Debian DSA-5588-1 : putty - security update]	high
12/24/2023	[Fedora 38 : xorg-x11-server-Xwayland (2023-77c8903bcb)]	high
12/24/2023	[Fedora 38 : mingw-gstreamer1 / mingw-gstreamer1-plugins-bad-free / etc (2023-0984b63b23)]	high
12/23/2023	[openSUSE 15 Security Update : tinysql (SUSE-SU-2023:4958-1)]	high
12/23/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xorg-x11-server (SUSE-SU-2023:4949-1)]	high
12/23/2023	[Fedora 39 : thunderbird (2023-7dee358171)]	high
12/23/2023	[SUSE SLES15 Security Update : gstreamer-plugins-bad (SUSE-SU-2023:4947-1)]	high
12/23/2023	[GLSA-202312-12 : Flatpak: Multiple Vulnerabilities]	high
12/23/2023	[GLSA-202312-10 : Ceph: Root Privilege Escalation]	high
12/23/2023	[Fedora 38 : filezilla / libfilezilla (2023-7934efb5e3)]	high
12/23/2023	[Debian DLA-3693-1 : opensslsigncode - LTS security update]	high
12/23/2023	[Fedora 38 : chromium (2023-ed327967b4)]	high
12/22/2023	[CentOS 7 : thunderbird (RHSA-2023:4945)]	high
12/22/2023	[CentOS 7 : insights-client (RHSA-2023:6795)]	high
12/22/2023	[CentOS 7 : xorg-x11-server (RHSA-2023:6802)]	high
12/22/2023	[CentOS 7 : firefox (RHSA-2023:4079)]	high
12/22/2023	[CentOS 7 : tigervnc and xorg-x11-server (RHSA-2023:1594)]	high
12/22/2023	[CentOS 7 : kernel (RHSA-2023:7423)]	high
12/22/2023	[CentOS 7 : thunderbird (RHSA-2023:7505)]	high
12/22/2023	[CentOS 7 : open-vm-tools (RHSA-2023:5217)]	high
12/22/2023	[CentOS 7 : squid (RHSA-2023:6805)]	high
12/22/2023	[CentOS 7 : subscription-manager (RHSA-2023:4701)]	high
12/22/2023	[CentOS 7 : firefox (RHSA-2023:3137)]	high
12/22/2023	[CentOS 7 : bind (RHSA-2023:5691)]	high
12/22/2023	[CentOS 7 : kernel (RHSA-2023:5622)]	high
12/22/2023	[Slackware Linux 15.0 / current postfix Vulnerability (SSA:2023-356-01)]	high
12/22/2023	[Siemens Industrial Products (CVE-2019-8460)]	high
12/22/2023	[Siemens Industrial Products Uncontrolled Resource Consumption (CVE-2019-11477)]	high
12/22/2023	[Siemens Industrial Products Uncontrolled Resource Consumption (CVE-2019-11479)]	high
12/22/2023	[Siemens Industrial Products Uncontrolled Resource Consumption (CVE-2019-11478)]	high

# Aktiv ausgenutzte Sicherheitslücken

## Exploits der letzten 5 Tage

“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](#)

---

” “Wed, 13 Dec 2023

### ***PDF24 Creator 11.15.1 Local Privilege Escalation***

PDF24 Creator versions 11.15.1 and below suffer from a local privilege escalation vulnerability via the MSI installer.

- [Link](#)

---

” “Wed, 13 Dec 2023

### ***One Identity Password Manager Kiosk Escape Privilege Escalation***

One Identity Password Manager versions prior to 5.13.1 suffer from a kiosk escape privilege escalation vulnerability.

- [Link](#)

---

” “Wed, 13 Dec 2023

### ***Atos Unify OpenScape Authentication Bypass / Remote Code Execution***

Atos Unify OpenScape Session Border Controller (SBC) versions before V10 R3.4.0, Branch versions before V10 R3.4.0, and BCF versions before V10 R10.12.00 and V10 R11.05.02 suffer from an argument injection vulnerability that can lead to unauthenticated remote code execution and authentication bypass.

- [Link](#)

---

” “Wed, 13 Dec 2023

### ***Anveo Mobile User Enumeration / Missing Certificate Validation***

Anveo Mobile application version 10.0.0.359 and server version 11.0.0.5 suffer from missing certificate validation and user enumeration vulnerabilities.

- [Link](#)

---

” “Tue, 12 Dec 2023

### ***Splunk XSLT Upload Remote Code Execution***

This Metasploit module exploits a remote code execution vulnerability in Splunk Enterprise. The affected versions include 9.0.x before 9.0.7 and 9.1.x before 9.1.2. The exploitation process leverages a weakness in the XSLT transformation functionality of Splunk. Successful exploitation requires valid credentials, typically admin:changeme by default. The exploit involves uploading a malicious XSLT file to the target system. This file, when processed by the vulnerable Splunk server, leads to the execution of arbitrary code. The module then utilizes the runshellscript capability in Splunk to execute the payload, which can be tailored to establish a reverse shell. This provides the attacker with remote control over the compromised Splunk instance. The module is designed to work seamlessly, ensuring successful exploitation under the right conditions.

- [Link](#)

---

” “Tue, 12 Dec 2023

### ***WordPress Backup Migration 1.3.7 Remote Code Execution***

WordPress Backup Migration plugin versions 1.3.7 and below suffer from a remote code execution vulnerability.

- [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
2023-12-21	Le département de l'Urbanisme et du Logement de Madhya Pradesh (Inde).	[IND]	<a href="#">Link</a>
2023-12-20	Kitco	[CAN]	<a href="#">Link</a>
2023-12-20	First American	[USA]	<a href="#">Link</a>
2023-12-19	HCL Technologies	[IND]	<a href="#">Link</a>
2023-12-19	St Vincent's Health Australia	[AUS]	<a href="#">Link</a>
2023-12-19	Liberty Hospital.	[USA]	<a href="#">Link</a>
2023-12-18	Elektroprivreda Srbije (EPS)	[SRB]	<a href="#">Link</a>
2023-12-17	Socadis	[CAN]	<a href="#">Link</a>
2023-12-16	Confédération Luxembourgeoise des Syndicats (LCGB)	[LUX]	<a href="#">Link</a>
2023-12-14	Verocard	[BRA]	<a href="#">Link</a>
2023-12-13	Limburg.net	[BEL]	<a href="#">Link</a>
2023-12-13	London Public Library	[CAN]	<a href="#">Link</a>
2023-12-13	Agência Nacional de Águas e Saneamento Básico (ANA)	[BRA]	<a href="#">Link</a>
2023-12-13	VF Corp	[USA]	<a href="#">Link</a>
2023-12-13	MongoDB	[USA]	<a href="#">Link</a>
2023-12-13	Western Railway's Lower Parel workshop	[IND]	<a href="#">Link</a>
2023-12-12	District de March	[CHE]	<a href="#">Link</a>
2023-12-12	Hotelplan UK	[GBR]	<a href="#">Link</a>
2023-12-11	Banque centrale du Lesotho	[LSO]	<a href="#">Link</a>
2023-12-11	Milton Town School District (MTSD)	[USA]	<a href="#">Link</a>
2023-12-10	Jysk Energi	[DNK]	<a href="#">Link</a>
2023-12-10	EasyPark	[NLD]	<a href="#">Link</a>
2023-12-10	CACG (Compagnie d'Aménagement des Coteaux de Gascogne)	[FRA]	<a href="#">Link</a>
2023-12-09	Mairie d'Ozoir-la-Ferrière	[FRA]	<a href="#">Link</a>
2023-12-08	Province des îles Loyauté	[NCL]	<a href="#">Link</a>
2023-12-08	WestPole	[ITA]	<a href="#">Link</a>
2023-12-08	Coaxis	[FRA]	<a href="#">Link</a>
2023-12-08	Kaunas University of Technology (KTU)	[LTU]	<a href="#">Link</a>
2023-12-07	Aqualectra	[CUW]	<a href="#">Link</a>
2023-12-07	Université de Wollongong	[AUS]	<a href="#">Link</a>
2023-12-07	Prefeitura de Poços de Caldas	[BRA]	<a href="#">Link</a>
2023-12-07	Hinsdale School District	[USA]	<a href="#">Link</a>
2023-12-06	Nissan Oceania	[AUS]	<a href="#">Link</a>
2023-12-06	Gouvernement du Yucatan	[MEX]	<a href="#">Link</a>
2023-12-06	Université de Sherbrooke	[CAN]	<a href="#">Link</a>
2023-12-06	Glendale Unified School District	[USA]	<a href="#">Link</a>
2023-12-06	Groveport Madison School District	[USA]	<a href="#">Link</a>
2023-12-05	Dameron Hospital	[USA]	<a href="#">Link</a>
2023-12-05	Gräbener Maschinentechnik	[DEU]	<a href="#">Link</a>
2023-12-04	Caribbean Community (Caricom) Secretariat	[GUY]	<a href="#">Link</a>
2023-12-01	Communauté de communes du Pays du Neubourg	[FRA]	<a href="#">Link</a>

## Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-26	[carolinalemke.com]	toufan	<a href="#">Link</a>
2023-12-26	[ari.co.il]	toufan	<a href="#">Link</a>
2023-12-26	[Abdali Hospital]	rhysida	<a href="#">Link</a>
2023-12-26	[Tshwane University of Technology]	rhysida	<a href="#">Link</a>
2023-12-25	[Blaine County Schools]	blacksuit	<a href="#">Link</a>
2023-12-25	[pcmarket.uz]	stormous	<a href="#">Link</a>
2023-12-25	[International Electronic Machines Corp]	akira	<a href="#">Link</a>
2023-12-25	[co.pickens.sc.us]	lockbit3	<a href="#">Link</a>
2023-12-25	[walkro.eu]	lockbit3	<a href="#">Link</a>
2023-12-25	[ontariopork.on.ca]	lockbit3	<a href="#">Link</a>
2023-12-25	[zrvp.ro]	lockbit3	<a href="#">Link</a>
2023-12-25	[tecnifibre.com]	lockbit3	<a href="#">Link</a>
2023-12-25	[hendelsinc.com]	lockbit3	<a href="#">Link</a>
2023-12-20	[Horizon Pool and Spa]	8base	<a href="#">Link</a>
2023-12-20	[Davis Cedillo and Mendoza Inc]	8base	<a href="#">Link</a>
2023-12-24	[Ono Academic College]	malekteam	<a href="#">Link</a>
2023-12-24	[dorimedia]	malekteam	<a href="#">Link</a>
2023-12-24	[gav.co.il]	malekteam	<a href="#">Link</a>
2023-12-24	[ZIV Hospital]	malekteam	<a href="#">Link</a>
2023-12-24	[Prefeitura Municipal de Itabira]	alphv	<a href="#">Link</a>
2023-12-24	[bkf-fleuren.de]	lockbit3	<a href="#">Link</a>
2023-12-23	[avescorent.ch]	lockbit3	<a href="#">Link</a>
2023-12-23	[allot.com]	toufan	<a href="#">Link</a>
2023-12-23	[Bay Orthopedic & Rehabilitation Supply]	bianlian	<a href="#">Link</a>
2023-12-15	[forabank.ru]	werewolves	<a href="#">Link</a>
2023-12-17	[vasexperts.ru]	werewolves	<a href="#">Link</a>
2023-12-23	[zurcherodioraven.com]	lockbit3	<a href="#">Link</a>
2023-12-23	[quakerwindows.com]	cactus	<a href="#">Link</a>
2023-12-23	[bconnect.co.il]	toufan	<a href="#">Link</a>
2023-12-23	[super-pharm.co.il]	toufan	<a href="#">Link</a>
2023-12-23	[PriceSmart (Update)]	alphv	<a href="#">Link</a>
2023-12-23	[castores.com.mx]	lockbit3	<a href="#">Link</a>
2023-12-22	[VF Corporation]	alphv	<a href="#">Link</a>
2023-12-22	[ciasc.mx]	lockbit3	<a href="#">Link</a>
2023-12-22	[csmsa.com.ar]	lockbit3	<a href="#">Link</a>
2023-12-22	[whafh.com]	blackbasta	<a href="#">Link</a>
2023-12-22	[hotelplan.co.uk]	blackbasta	<a href="#">Link</a>
2023-12-22	[Nissan Australia]	akira	<a href="#">Link</a>
2023-12-22	[xeinadin.com]	lockbit3	<a href="#">Link</a>
2023-12-22	[igs-inc.com]	lockbit3	<a href="#">Link</a>
2023-12-22	[teldor.com]	toufan	<a href="#">Link</a>
2023-12-22	[erco.co.il]	toufan	<a href="#">Link</a>
2023-12-22	[esepac.com]	lockbit3	<a href="#">Link</a>
2023-12-22	[fager-mcgee.com]	lockbit3	<a href="#">Link</a>
2023-12-22	[goldenc.com]	lockbit3	<a href="#">Link</a>
2023-12-22	[sterlinghomes.com.au]	lockbit3	<a href="#">Link</a>
2023-12-22	[denford.co.uk]	lockbit3	<a href="#">Link</a>
2023-12-21	[comtrade.com]	stormous	<a href="#">Link</a>
2023-12-21	[zewailcity.edu.eg]	stormous	<a href="#">Link</a>
2023-12-21	[evn.com.vn]	stormous	<a href="#">Link</a>
2023-12-21	[inwi.ma]	stormous	<a href="#">Link</a>
2023-12-21	[rmutto.ac.th]	stormous	<a href="#">Link</a>
2023-12-21	[trabzon.edu.tr]	stormous	<a href="#">Link</a>
2023-12-21	[ACE Air Cargo]	dragonforce	<a href="#">Link</a>
2023-12-21	[Kinetic Leasing]	dragonforce	<a href="#">Link</a>
2023-12-13	[dillarddoor.com]	cactus	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-16	[cts.co.uk]	cactus	<a href="#">Link</a>
2023-12-20	[hunterbuildings.com]	cactus	<a href="#">Link</a>
2023-12-20	[larlyn.com]	cactus	<a href="#">Link</a>
2023-12-20	[wkw-group.com]	cactus	<a href="#">Link</a>
2023-12-20	[dbmgroupp.com]	cactus	<a href="#">Link</a>
2023-12-20	[Jon Richard]	play	<a href="#">Link</a>
2023-12-20	[Concept Data]	play	<a href="#">Link</a>
2023-12-20	[Packaging Solutions]	play	<a href="#">Link</a>
2023-12-21	[Owen Quilty Professional]	play	<a href="#">Link</a>
2023-12-21	[zonesoft.pt]	stormous	<a href="#">Link</a>
2023-12-21	[zonesoft.pt]	ranstreet	<a href="#">Link</a>
2023-12-20	[Yakult Australia]	dragonforce	<a href="#">Link</a>
2023-12-20	[Bladen County Public Library]	meow	<a href="#">Link</a>
2023-12-20	[smudlers.com]	lockbit3	<a href="#">Link</a>
2023-12-20	[Unite Here]	incransom	<a href="#">Link</a>
2023-12-20	[tefentech.com]	toufan	<a href="#">Link</a>
2023-12-20	[zoko.co.il]	toufan	<a href="#">Link</a>
2023-12-20	[Di Martino Group ]	ragroup	<a href="#">Link</a>
2023-12-20	[Rockford Gastroenterology Associates ]	ragroup	<a href="#">Link</a>
2023-12-20	[HALLIDAYS GROUP LIMITED ]	ragroup	<a href="#">Link</a>
2023-12-20	[Die Unfallkasse Thüringen ]	ragroup	<a href="#">Link</a>
2023-12-20	[NIDEC GPM GmbH ]	ragroup	<a href="#">Link</a>
2023-12-20	[dobsystems.com]	lockbit3	<a href="#">Link</a>
2023-12-20	[des-igngroup.com]	lockbit3	<a href="#">Link</a>
2023-12-20	[Navigation Financial Group]	alphv	<a href="#">Link</a>
2023-12-20	[udhaiyamdhall.com]	lockbit3	<a href="#">Link</a>
2023-12-20	[Air Sino-Euro Associates Travel Pte. Ltd]	bianlian	<a href="#">Link</a>
2023-12-20	[LCGB]	8base	<a href="#">Link</a>
2023-12-20	[CETEC Ingénierie]	8base	<a href="#">Link</a>
2023-12-20	[The International School of Management]	8base	<a href="#">Link</a>
2023-12-20	[Employ Milwaukee]	8base	<a href="#">Link</a>
2023-12-20	[Horizon Pool & Spa]	8base	<a href="#">Link</a>
2023-12-20	[socadis]	8base	<a href="#">Link</a>
2023-12-20	[Davis Cedillo & Mendoza Inc]	8base	<a href="#">Link</a>
2023-12-20	[spiritleatherworks.com]	lockbit3	<a href="#">Link</a>
2023-12-19	[strauss-group.com]	toufan	<a href="#">Link</a>
2023-12-19	[RCSB PDB]	meow	<a href="#">Link</a>
2023-12-19	[mtsd-vt.org]	lockbit3	<a href="#">Link</a>
2023-12-19	[Viking Therapeutics]	alphv	<a href="#">Link</a>
2023-12-19	[www.pts-tools.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.plasson-pead.com.br]	toufan	<a href="#">Link</a>
2023-12-19	[www.nistx.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.ktstooling.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.herrickindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.drillmex.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.dixie-tool.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.copreinternacional.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.butlerbros.com]	toufan	<a href="#">Link</a>
2023-12-19	[www.atwoodindustries.com]	toufan	<a href="#">Link</a>
2023-12-19	[wsies.com]	toufan	<a href="#">Link</a>
2023-12-19	[vehicle.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[tryhardindustrial.ca]	toufan	<a href="#">Link</a>
2023-12-19	[sys.udidagan.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[sys.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[sys-cspartnershq1.caesarstone.com]	toufan	<a href="#">Link</a>
2023-12-19	[sys-cspartners.caesarstoneus.com]	toufan	<a href="#">Link</a>
2023-12-19	[sys-cspartners.caesarstone.sg]	toufan	<a href="#">Link</a>
2023-12-19	[sys-cspartners.caesarstone.co.uk]	toufan	<a href="#">Link</a>
2023-12-19	[sys-cspartners.caesarstone.com.au]	toufan	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-19	[sys-cspartners.caesarstone.ca]	toufan	<a href="#">Link</a>
2023-12-19	[sys.biopet.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[store.toolneeds.com]	toufan	<a href="#">Link</a>
2023-12-19	[store.brunswickindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[stage.kravitz.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[shop.smithindustrialsupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[shop.shopsupply.net]	toufan	<a href="#">Link</a>
2023-12-19	[shop.reggiemckenzieindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[shop.qct.tools]	toufan	<a href="#">Link</a>
2023-12-19	[shop.lgindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[shop.emprecise.com]	toufan	<a href="#">Link</a>
2023-12-19	[shop.clador.com]	toufan	<a href="#">Link</a>
2023-12-19	[shop.britecon.com]	toufan	<a href="#">Link</a>
2023-12-19	[shefa-online.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[selwayindustrialsupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[rocket-supply.com]	toufan	<a href="#">Link</a>
2023-12-19	[rmpis.com]	toufan	<a href="#">Link</a>
2023-12-19	[reserved-il.com]	toufan	<a href="#">Link</a>
2023-12-19	[pts-tools.com]	toufan	<a href="#">Link</a>
2023-12-19	[product.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[pmt-usa.com]	toufan	<a href="#">Link</a>
2023-12-19	[phoenix.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[pet.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[pet.biopet.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[paragon-supply.com]	toufan	<a href="#">Link</a>
2023-12-19	[old.shefa-online.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[norviktools.com]	toufan	<a href="#">Link</a>
2023-12-19	[northernprecisionsales.com]	toufan	<a href="#">Link</a>
2023-12-19	[newstore.johnstoncompanies.com]	toufan	<a href="#">Link</a>
2023-12-19	[mortgage.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[morsecuttingtools.com]	toufan	<a href="#">Link</a>
2023-12-19	[mitchellmckinney.com]	toufan	<a href="#">Link</a>
2023-12-19	[mgisales.com]	toufan	<a href="#">Link</a>
2023-12-19	[m.biopet.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[libertytool.com]	toufan	<a href="#">Link</a>
2023-12-19	[ktstooling.com]	toufan	<a href="#">Link</a>
2023-12-19	[knightesupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[keter.com]	toufan	<a href="#">Link</a>
2023-12-19	[keter.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[its-supply.com]	toufan	<a href="#">Link</a>
2023-12-19	[h-o.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[goronco.com]	toufan	<a href="#">Link</a>
2023-12-19	[gordonindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[global.keter.com]	toufan	<a href="#">Link</a>
2023-12-19	[giddirect.com]	toufan	<a href="#">Link</a>
2023-12-19	[gfwdsupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[fugatesales.com]	toufan	<a href="#">Link</a>
2023-12-19	[drillmex.com]	toufan	<a href="#">Link</a>
2023-12-19	[dixie-tool.com]	toufan	<a href="#">Link</a>
2023-12-19	[dctsupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[cspartnershq1.caesarstone.com]	toufan	<a href="#">Link</a>
2023-12-19	[cspartners.caesarstoneus.com]	toufan	<a href="#">Link</a>
2023-12-19	[cspartners.caesarstone.sg]	toufan	<a href="#">Link</a>
2023-12-19	[cspartners.caesarstone.co.uk]	toufan	<a href="#">Link</a>
2023-12-19	[cspartners.caesarstone.com.au]	toufan	<a href="#">Link</a>
2023-12-19	[cspartners.caesarstone.ca]	toufan	<a href="#">Link</a>
2023-12-19	[core.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[copreinternacional.com]	toufan	<a href="#">Link</a>
2023-12-19	[colmarindustrial.com]	toufan	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-19	[cmtindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[cdt1.com]	toufan	<a href="#">Link</a>
2023-12-19	[catalog.ustg.net]	toufan	<a href="#">Link</a>
2023-12-19	[catalog.toolkrib.com]	toufan	<a href="#">Link</a>
2023-12-19	[catalog.fotcnc.com]	toufan	<a href="#">Link</a>
2023-12-19	[cartersoshkosh.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[butlerbros.com]	toufan	<a href="#">Link</a>
2023-12-19	[blueashsupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[berkshiresupply.com]	toufan	<a href="#">Link</a>
2023-12-19	[barindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[badgermill.com]	toufan	<a href="#">Link</a>
2023-12-19	[atwoodindustries.com]	toufan	<a href="#">Link</a>
2023-12-19	[arieladar.com]	toufan	<a href="#">Link</a>
2023-12-19	[api.touch-ins.co.il]	toufan	<a href="#">Link</a>
2023-12-19	[apisinc.com]	toufan	<a href="#">Link</a>
2023-12-19	[amtektool.com]	toufan	<a href="#">Link</a>
2023-12-19	[allegHENYtool.net]	toufan	<a href="#">Link</a>
2023-12-19	[alcornindustrial.com]	toufan	<a href="#">Link</a>
2023-12-19	[ustg.net]	toufan	<a href="#">Link</a>
2023-12-19	[chuzefitness.com]	lockbit3	<a href="#">Link</a>
2023-12-19	[brintons.co.uk]	blackbasta	<a href="#">Link</a>
2023-12-19	[pecofoods.com]	blackbasta	<a href="#">Link</a>
2023-12-19	[Kauno Technologijos Universitetas]	rhysida	<a href="#">Link</a>
2023-12-18	[Blackstone Valley Community Health Care]	hunters	<a href="#">Link</a>
2023-12-18	[Richard Harris Personal Injury Law Firm]	play	<a href="#">Link</a>
2023-12-18	[Schoepe Display]	play	<a href="#">Link</a>
2023-12-18	[Waldner's]	play	<a href="#">Link</a>
2023-12-18	[Succes Schoonmaak]	play	<a href="#">Link</a>
2023-12-18	[DYWIDAG-Systems & American Transportation]	play	<a href="#">Link</a>
2023-12-18	[C????z????]	play	<a href="#">Link</a>
2023-12-18	[The CM Paula]	play	<a href="#">Link</a>
2023-12-18	[parat-technology.com]	lockbit3	<a href="#">Link</a>
2023-12-18	[Viking Therapeutics reported to the SEC following a breach]	alphv	<a href="#">Link</a>
2023-12-18	[naandanjain.com]	toufan	<a href="#">Link</a>
2023-12-18	[LAJOLLAGROUP]	cactus	<a href="#">Link</a>
2023-12-18	[Ta-Supply.com]	toufan	<a href="#">Link</a>
2023-12-18	[Electrical Connections]	bianlian	<a href="#">Link</a>
2023-12-18	[navitaspets.com]	blackbasta	<a href="#">Link</a>
2023-12-18	[vyera.com]	blackbasta	<a href="#">Link</a>
2023-12-18	[hallidays.co.uk]	blackbasta	<a href="#">Link</a>
2023-12-17	[techno-rezef.com]	toufan	<a href="#">Link</a>
2023-12-17	[curver.com]	toufan	<a href="#">Link</a>
2023-12-17	[dorot.com]	toufan	<a href="#">Link</a>
2023-12-17	[graf.co.il]	toufan	<a href="#">Link</a>
2023-12-17	[brother.co.il]	toufan	<a href="#">Link</a>
2023-12-17	[ATCO Products Inc]	medusa	<a href="#">Link</a>
2023-12-17	[Biomatrix LLC]	medusa	<a href="#">Link</a>
2023-12-17	[TechKids aka MindX]	raznatovic	<a href="#">Link</a>
2023-12-17	[SKF.com]	raznatovic	<a href="#">Link</a>
2023-12-17	[Colonial Pipeline]	raznatovic	<a href="#">Link</a>
2023-12-17	[rodo.co.uk]	lockbit3	<a href="#">Link</a>
2023-12-16	[E & J Gallo Winery]	alphv	<a href="#">Link</a>
2023-12-14	[Kraft Foods]	snatch	<a href="#">Link</a>
2023-12-14	[Spaulding Clinical]	snatch	<a href="#">Link</a>
2023-12-16	[Crace Medical Centre]	knight	<a href="#">Link</a>
2023-12-16	[DSG-US.COM]	clon	<a href="#">Link</a>
2023-12-16	[New York School of Interior Design]	incransom	<a href="#">Link</a>
2023-12-16	[CTS]	cactus	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-16	[kohlwholesale.com]	blackbasta	Link
2023-12-16	[Insidesource]	8base	Link
2023-12-15	[hebeler.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	[converzamedia.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	[grandrapidsomenshealth.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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-13	[Hawkins Sales]	8base	<a href="#">Link</a>
2023-12-13	[William Jackson Food Group]	8base	<a href="#">Link</a>
2023-12-13	[Groupe PROMOBÉ]	8base	<a href="#">Link</a>
2023-12-13	[Soethoudt metaalbewerking b.v.]	8base	<a href="#">Link</a>
2023-12-13	[REUS MOBILITAT I SERVEIS]	8base	<a href="#">Link</a>
2023-12-13	[Tim Davies Landscaping]	8base	<a href="#">Link</a>
2023-12-12	[King Aerospace, Inc.]	incransom	<a href="#">Link</a>
2023-12-12	[GlobalSpec]	play	<a href="#">Link</a>
2023-12-12	[dena.de]	lockbit3	<a href="#">Link</a>
2023-12-12	[woodruffenterprises.com]	threeam	<a href="#">Link</a>
2023-12-12	[shareharris.com]	threeam	<a href="#">Link</a>
2023-12-12	[SmartWave Technologies]	akira	<a href="#">Link</a>
2023-12-12	[Mitrani Caballero Ojam & Ruiz Moreno - Abogados]	akira	<a href="#">Link</a>
2023-12-12	[The Teaching Company, LLC]	akira	<a href="#">Link</a>
2023-12-12	[Memorial Sloan Kettering Cancer Center]	meow	<a href="#">Link</a>
2023-12-12	[petrotec.com.qa]	lockbit3	<a href="#">Link</a>
2023-12-12	[tradewindscorp-insbrok.com]	lockbit3	<a href="#">Link</a>
2023-12-12	[airtechthelong.com.vn]	lockbit3	<a href="#">Link</a>
2023-12-12	[kitahirosima.jp]	lockbit3	<a href="#">Link</a>
2023-12-12	[Grupo Jose Alves]	rhysida	<a href="#">Link</a>
2023-12-12	[Insomniac Games]	rhysida	<a href="#">Link</a>
2023-12-11	[phillipsglobal.us]	lockbit3	<a href="#">Link</a>
2023-12-11	[greenbriersportingclub.com]	lockbit3	<a href="#">Link</a>
2023-12-11	[ipp-sa.com]	lockbit3	<a href="#">Link</a>
2023-12-11	[r-ab.de]	lockbit3	<a href="#">Link</a>
2023-12-11	[Azienda USL di Modena]	hunters	<a href="#">Link</a>
2023-12-11	[igt.nl]	lockbit3	<a href="#">Link</a>
2023-12-01	[Bayer Heritage Federal Credit Union]	lorenz	<a href="#">Link</a>
2023-12-11	[MSD Information technology]	akira	<a href="#">Link</a>
2023-12-11	[Goiasa]	akira	<a href="#">Link</a>
2023-12-11	[Hinsdale School District ]	medusa	<a href="#">Link</a>
2023-12-11	[Independent Recovery Resources, Inc.]	bianlian	<a href="#">Link</a>
2023-12-11	[Studio MF]	akira	<a href="#">Link</a>
2023-12-11	[zailaboratory.com]	lockbit3	<a href="#">Link</a>
2023-12-11	[ISC Consulting Engineers]	cactus	<a href="#">Link</a>
2023-12-11	[The Glendale Unified School District]	medusa	<a href="#">Link</a>
2023-12-10	[pronatindustries.com]	lockbit3	<a href="#">Link</a>
2023-12-10	[policia.gob.pe]	lockbit3	<a href="#">Link</a>
2023-12-10	[Holding Slovenske elektrarne]	rhysida	<a href="#">Link</a>
2023-12-10	[Hse]	rhysida	<a href="#">Link</a>
2023-12-09	[Qatar Racing and Equestrian Club]	rhysida	<a href="#">Link</a>
2023-12-09	[Graphic Solutions Group Inc (US)]	daixin	<a href="#">Link</a>
2023-12-09	[OpTransRights - 2]	siegedsec	<a href="#">Link</a>
2023-12-09	[Telerad]	siegedsec	<a href="#">Link</a>
2023-12-09	[Technical University of Mombasa]	siegedsec	<a href="#">Link</a>
2023-12-09	[National Office for centralized procurement]	siegedsec	<a href="#">Link</a>
2023-12-09	[Portland Government & United states government]	siegedsec	<a href="#">Link</a>
2023-12-09	[Staples]	siegedsec	<a href="#">Link</a>
2023-12-09	[Deqing County]	siegedsec	<a href="#">Link</a>
2023-12-09	[Colombian National Registry]	siegedsec	<a href="#">Link</a>
2023-12-09	[HMW - Press Release]	monti	<a href="#">Link</a>
2023-12-08	[livanova.com]	lockbit3	<a href="#">Link</a>
2023-12-04	[Jerry Pate Energy (hack from Saltmarsh Financial Advisors)]	snatch	<a href="#">Link</a>
2023-12-08	[GOLFZON]	blacksuit	<a href="#">Link</a>
2023-12-08	[aw-lawyers.com]	lockbit3	<a href="#">Link</a>
2023-12-08	[midlandindustries.com]	lockbit3	<a href="#">Link</a>
2023-12-08	[Travian Games]	rhysida	<a href="#">Link</a>
2023-12-08	[Teman]	rhysida	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-07	[California Innovations]	play	<a href="#">Link</a>
2023-12-07	[SMRT]	play	<a href="#">Link</a>
2023-12-07	[Intrepid Sea, Air & Space Museum]	play	<a href="#">Link</a>
2023-12-07	[Postworks]	play	<a href="#">Link</a>
2023-12-07	[PLS Logistics]	play	<a href="#">Link</a>
2023-12-07	[Ridge Vineyards]	play	<a href="#">Link</a>
2023-12-07	[AJO]	play	<a href="#">Link</a>
2023-12-07	[PHIBRO GMBH]	play	<a href="#">Link</a>
2023-12-07	[denave.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[Precision Technologies Group Ltd]	incransom	<a href="#">Link</a>
2023-12-07	[Silvent North America]	play	<a href="#">Link</a>
2023-12-07	[GreenWaste Recovery]	play	<a href="#">Link</a>
2023-12-07	[Burton Wire & Cable]	play	<a href="#">Link</a>
2023-12-07	[Capespan]	play	<a href="#">Link</a>
2023-12-07	[Becker Furniture World]	play	<a href="#">Link</a>
2023-12-07	[Payne Hicks Beach]	play	<a href="#">Link</a>
2023-12-07	[Vitro Plus]	play	<a href="#">Link</a>
2023-12-07	[GVM]	play	<a href="#">Link</a>
2023-12-07	[Planbox]	play	<a href="#">Link</a>
2023-12-07	[AG Consulting Engineering]	play	<a href="#">Link</a>
2023-12-07	[Greater Richmond Transit]	play	<a href="#">Link</a>
2023-12-07	[Kuriyama of America]	play	<a href="#">Link</a>
2023-12-07	[bluewaterstt.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[omegapainclinic.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[AMCO Proteins]	bianlian	<a href="#">Link</a>
2023-12-07	[SML Group]	bianlian	<a href="#">Link</a>
2023-12-07	[stormtech]	metaencryptor	<a href="#">Link</a>
2023-12-07	[Garda]	metaencryptor	<a href="#">Link</a>
2023-12-07	[Tri-city Medical Center]	incransom	<a href="#">Link</a>
2023-12-07	[Tasteful Selections]	akira	<a href="#">Link</a>
2023-12-07	[Ware Manufacturing]	qilin	<a href="#">Link</a>
2023-12-07	[Neurology Center of Nevada]	qilin	<a href="#">Link</a>
2023-12-07	[CIE Automotive]	cactus	<a href="#">Link</a>
2023-12-07	[National Nail Corp]	cactus	<a href="#">Link</a>
2023-12-07	[citizenswv.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[directradiology.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[signiflow.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[bpce.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[hopto.com]	lockbit3	<a href="#">Link</a>
2023-12-07	[usherbrooke.ca]	lockbit3	<a href="#">Link</a>
2023-12-07	[Visan]	8base	<a href="#">Link</a>
2023-12-07	[Tryax Realty Management - Press Release]	monti	<a href="#">Link</a>
2023-12-06	[Campbell County Schools ]	medusa	<a href="#">Link</a>
2023-12-06	[Deutsche Energie-Agentur]	alphv	<a href="#">Link</a>
2023-12-06	[Compass Group Italia]	akira	<a href="#">Link</a>
2023-12-06	[Aqualectra Holdings]	akira	<a href="#">Link</a>
2023-12-06	[Acero Engineering]	bianlian	<a href="#">Link</a>
2023-12-06	[syrtech.com]	threeam	<a href="#">Link</a>
2023-12-06	[ACCU Reference Medical Lab]	medusa	<a href="#">Link</a>
2023-12-06	[Sagent]	medusa	<a href="#">Link</a>
2023-12-06	[fpz.com]	lockbit3	<a href="#">Link</a>
2023-12-06	[labelians.fr]	lockbit3	<a href="#">Link</a>
2023-12-06	[polyclinique-cotentin.com]	lockbit3	<a href="#">Link</a>
2023-12-06	[Lischkoff and Pitts, P.C.]	8base	<a href="#">Link</a>
2023-12-06	[SMG Confrere]	8base	<a href="#">Link</a>
2023-12-06	[Calgary TELUS Convention Centre]	8base	<a href="#">Link</a>
2023-12-06	[astley.]	8base	<a href="#">Link</a>
2023-12-05	[Henry Schein Inc - Henry's " LOST SHINE "]	alphv	<a href="#">Link</a>
2023-12-05	[TraCS Florida FSU]	alphv	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[Evnhcme]	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
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](https://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](mailto:info@cyberwald.com)

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