



Ausgabe: 20231222

# 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)

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

- [Link](#)

---

Thu, 21 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](#)

---

Thu, 21 Dec 2023

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

Ein entfernter, anonym 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 anonym 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, anonym 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](#)

---

Thu, 21 Dec 2023

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

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

- [Link](#)

---

Wed, 20 Dec 2023

***[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen***

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

- [Link](#)

---

Wed, 20 Dec 2023

***[NEU] [hoch] Dell BIOS: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff***

Ein lokaler Angreifer kann mehrere Schwachstellen in Dell BIOS ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

---

Wed, 20 Dec 2023

***[UPDATE] [hoch] MediaWiki: Mehrere Schwachstellen ermöglichen Codeausführung***

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in MediaWiki ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Wed, 20 Dec 2023

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

---

Wed, 20 Dec 2023

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

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

- [Link](#)

---

Tue, 19 Dec 2023

***[UPDATE] [kritisch] Perl: Schwachstelle ermöglicht Privilegieneskalation***

Ein Angreifer kann eine Schwachstelle in Perl ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Tue, 19 Dec 2023

***[UPDATE] [hoch] Perl: Mehrere Schwachstellen ermöglichen Codeausführung***

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Perl ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 19 Dec 2023

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

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

- [Link](#)

---

Tue, 19 Dec 2023

***[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten***

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

- [Link](#)

---

Tue, 19 Dec 2023

***[UPDATE] [hoch] Apache Struts: Schwachstelle ermöglicht Denial of Service***

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

- [Link](#)

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/21/2023	[SUSE SLES15 Security Update : openssh (SUSE-SU-2023:4905-1)]	critical
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssh (SUSE-SU-2023:4902-1)]	critical
12/21/2023	[SUSE SLES15 Security Update : openssh (SUSE-SU-2023:4904-1)]	critical
12/21/2023	[FreeBSD : chromium – security fix (1b2a8e8a-9fd5-11ee-86bb-a8a1599412c6)]	critical
12/21/2023	[Nagios XI < 5.11.3 Multiple Vulnerabilities]	critical
12/21/2023	[Ivanti Avalanche Unauthenticated Stack-based Buffer Overflow (CVE-2023-46216)]	critical
12/21/2023	[Cisco Identity Services Engine RCE (cisco-sa-struts-C2kCMkmT)]	critical
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.21-openssl (SUSE-SU-2023:4931-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libreoffice (SUSE-SU-2023:4932-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xwayland (SUSE-SU-2023:4926-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2023:4928-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.20-openssl (SUSE-SU-2023:4930-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xorg-x11-server (SUSE-SU-2023:4925-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ghostscript (SUSE-SU-2023:4920-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xorg-x11-server (SUSE-SU-2023:4934-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xwayland (SUSE-SU-2023:4933-1)]	high
12/21/2023	[SUSE SLES15 Security Update : MozillaFirefox (SUSE-SU-2023:4929-1)]	high
12/21/2023	[Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities]	high
12/21/2023	[AIX 7.3 TL 1 : printers (IJ48539)]	high
12/21/2023	[AIX 7.2 TL 5 : bind (IJ44424)]	high
12/21/2023	[AIX 7.3 TL 0 : printers (IJ48784)]	high
12/21/2023	[AIX 7.2 TL 5 : printers (IJ48481)]	high
12/21/2023	[AIX 7.2 TL 5 : bind (IJ49093)]	high
12/21/2023	[AIX 7.3 TL 0 : aixwindows (IJ48758)]	high
12/21/2023	[AIX 7.3 TL 1 : aixwindows (IJ48540)]	high
12/21/2023	[SUSE SLES12 Security Update : ghostscript (SUSE-SU-2023:4917-1)]	high
12/21/2023	[SUSE SLES15 Security Update : gstreamer-plugins-bad (SUSE-SU-2023:4944-1)]	high
12/21/2023	[SUSE SLES12 Security Update : xorg-x11-server (SUSE-SU-2023:4935-1)]	high
12/21/2023	[SUSE SLED15 / SLES15 Security Update : gstreamer-plugins-bad (SUSE-SU-2023:4943-1)]	high
12/21/2023	[Oracle Linux 8 : postgresql:15 (ELSA-2023-7884)]	high
12/21/2023	[Microsoft Edge (Chromium) < 120.0.2210.91 (CVE-2023-7024)]	high

Datum	Schwachstelle	Bewertung
12/21/2023	[FreeBSD : gitea – Prefix Truncation Attack against ChaCha20-Poly1305 and Encrypt-then-MAC aka Terrapin (b2765c89-a052-11ee-bed2-596753f1a87c)]	high
12/20/2023	[Cisco IOS and NX-OS Software Locator/ID Separation Protocol Packet DOS (CVE-2016-1351)]	high
12/20/2023	[ABB Relion Improper Input Validation (CVE-2023-4518)]	high



# Aktiv ausgenutzte Sicherheitslücken

## Exploits der letzten 5 Tage

“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](#)

---

” “Mon, 11 Dec 2023

***WordPress Contact Form To Any API 1.1.6 Cross Site Request Forgery***

WordPress Contact Form to Any API plugin versions 1.1.6 and below suffer from a cross site request forgery vulnerability.

- [Link](#)

---

” “Mon, 11 Dec 2023

***WordPress Bravo Translate 1.2 SQL Injection***

WordPress Bravo Translate plugin versions 1.2 and below suffer from a remote SQL injection vulnerability.

- [Link](#)

---

” “Mon, 11 Dec 2023

***WordPress TextMe SMS 1.9.0 Cross Site Request Forgery***

WordPress TextMe SMS plugin versions 1.9.0 and below suffer from a cross site request forgery vulnerability.

- [Link](#)

---

”

## 0-Days der letzten 5 Tage

“Thu, 21 Dec 2023

***ZDI-23-1913: (0Day) Kofax Power PDF JP2 File Parsing Use-After-Free Information Disclosure Vulnerability***

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1912: (0Day) Kofax Power PDF JP2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1911: (0Day) Kofax Power PDF JP2 File Parsing Use-After-Free Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1910: (0Day) Kofax Power PDF JP2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1909: (0Day) Kofax Power PDF J2K File Parsing Memory Corruption Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1908: (0Day) Kofax Power PDF PNG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1907: (0Day) Kofax Power PDF U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1906: (0Day) Kofax Power PDF U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1905: (0Day) BlueZ Audio Profile AVRCP parse\_media\_folder Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1904: (0Day) BlueZ Audio Profile AVRCP parse\_media\_element Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1903: (0Day) BlueZ Audio Profile AVRCP avrcp\_parse\_attribute\_list Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1902: (0Day) BlueZ Phone Book Access Profile Heap-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1901: (0Day) BlueZ OBEX Library Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1900: (0Day) BlueZ Audio Profile AVRCP Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1899: Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Thu, 21 Dec 2023

*ZDI-23-1898: Rockwell Automation Arena Simulation DOE File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1897: (0Day) Voltronic Power ViewPower Pro selectDeviceListBy SQL Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1896: (0Day) Voltronic Power ViewPower Pro Expression Language Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1895: (0Day) Voltronic Power ViewPower Pro doDocument XML External Entity Processing Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1894: (0Day) Voltronic Power ViewPower Pro UpLoadAction Unrestricted File Upload Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1893: (0Day) Voltronic Power ViewPower Pro MySQL Use of Hard-coded Credentials Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1892: (0Day) Voltronic Power ViewPower getModbusPassword Missing Authentication Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1891: (0Day) Voltronic Power ViewPower Pro selectEventConfig SQL Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1890: (0Day) Voltronic Power ViewPower USBCommEx shutdown Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1889: (0Day) Voltronic Power ViewPower USBCommEx shutdown Exposed Dangerous Method Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1888: (0Day) Voltronic Power ViewPower UpsScheduler Exposed Dangerous Method Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1887: (0Day) Voltronic Power ViewPower LinuxMonitorConsole Exposed Dangerous Method Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1886: (0Day) Voltronic Power ViewPower MacMonitorConsole Exposed Dangerous Method Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1885: (0Day) Voltronic Power ViewPower Incorrect Permission Assignment Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1884: (0Day) Voltronic Power ViewPower MonitorConsole Exposed Dangerous Method Denial-of-Service Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1883: (0Day) Voltronic Power ViewPower setShutdown Exposed Dangerous Method Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1882: (0Day) Voltronic Power ViewPower Deserialization of Untrusted Data Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1881: (0Day) Voltronic Power ViewPower MonitorConsole Exposed Dangerous Method Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1880: (0Day) Voltronic Power ViewPower updateManagerPassword Exposed Dangerous Method Authentication Bypass Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1879: (0Day) Voltronic Power ViewPower Pro updateManagerPassword Exposed Dangerous Function Authentication Bypass Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1878: (0Day) Voltronic Power ViewPower Pro getMacAddressByIp Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1877: (0Day) Voltronic Power ViewPower Pro SocketService Missing Authentication Denial-of-Service Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1876: (0Day) Voltronic Power ViewPower Pro Deserialization of Untrusted Data Re-*

*mote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1875: Foxit PDF Reader AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1874: Foxit PDF Reader Annotation Type Confusion Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1873: Foxit PDF Reader AcroForm Signature Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1872: Foxit PDF Reader Doc Out-Of-Bounds Read Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1871: Foxit PDF Reader AcroForm Doc Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1870: Foxit PDF Reader AcroForm Doc Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1869: Foxit PDF Reader AcroForm Doc Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1868: Foxit PDF Reader Doc Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1867: Foxit PDF Reader Bookmark Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1866: Foxit PDF Reader Signature Use-After-Free Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1865: Foxit PDF Reader AcroForm Signature Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1864: Foxit PDF Reader combobox Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1863: Foxit PDF Reader AcroForm Doc Object Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1862: Foxit PDF Reader PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1861: oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1860: oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1859: oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1858: oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1857: (0Day) Hancom Office Show PPT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1856: (0Day) Hancom Office Cell XLS File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1855: (0Day) Hancom Office Word DOC File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1854: (0Day) Honeywell Saia PG5 Controls Suite XML External Entity Processing Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1853: (0Day) Honeywell Saia PG5 Controls Suite XML External Entity Processing Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1852: (0Day) Honeywell Saia PG5 Controls Suite CAB File Parsing Directory Traversal Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1851: (0Day) Honeywell Saia PG5 Controls Suite XML External Entity Processing In-*



*formation Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1850: (0Day) Honeywell Saia PG5 Controls Suite XML External Entity Processing Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1849: (0Day) Honeywell Saia PG5 Controls Suite XML External Entity Processing Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1848: (0Day) Honeywell Saia PG5 Controls Suite Directory Traversal Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1847: NETGEAR ProSAFE Network Management System saveNodeLabel Cross-Site Scripting Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1846: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1845: Trimble SketchUp Viewer SKP File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1844: Trimble SketchUp Viewer SKP File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1843: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1842: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1841: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1840: Trimble SketchUp Viewer SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1839: Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1838: Trimble SketchUp Viewer SKP File Parsing Uninitialized Variable Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1837: Trimble SketchUp Viewer SKP File Parsing Memory Corruption Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1836: Linux Mint Xreader CBT File Parsing Argument Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1835: Linux Mint Xreader EPUB File Parsing Directory Traversal Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1834: Linux Kernel nf\_tables\_expr\_destroy Use-After-Free Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1833: D-Link G416 awsfile rm Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1832: D-Link G416 awsfile tar File Handling Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1831: D-Link G416 nodered gz File Handling Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1830: D-Link G416 nodered tar File Handling Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1829: D-Link G416 nodered File Handling Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1828: D-Link G416 httpd Improper Handling of Exceptional Conditions Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1827: D-Link G416 httpd API-AUTH Timestamp Processing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1826: D-Link G416 httpd API-AUTH Digest Processing Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1825: D-Link G416 cfgsave Stack-Based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1824: D-Link G416 ovpnconf Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1823: D-Link G416 flupl filename Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1822: D-Link G416 flupl query\_type edit Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1821: D-Link G416 awsfile chmod Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1820: D-Link G416 flupl pythonapp Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1819: D-Link G416 nodered chmod Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1818: D-Link G416 flupl pythonmodules Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1817: D-Link G416 cfgsave upusb Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1816: D-Link G416 cfgsave backusb Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1815: D-Link G416 httpd Missing Authentication for Critical Function Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1814: D-Link G416 cfgsave Command Injection Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1813: Inductive Automation Ignition ModuleInvoke Deserialization of Untrusted Data Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1812: BlueZ Phone Book Access Profile Heap-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1811: BlueZ Phone Book Access Profile Heap-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 20 Dec 2023

*ZDI-23-1810: QEMU NVMe Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1809: TP-Link TL-WR902AC dm\_fillObjByStr Stack-based Buffer Overflow Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1808: TP-Link TL-WR841N dropbearpwd Improper Authentication Information Disclosure Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1807: X.Org Server Damage Object Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1806: X.Org Server Window Object Use-After-Free Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1805: Parallels Desktop Updater Link Following Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1804: Parallels Desktop virtio-gpu Out-Of-Bounds Write Remote Code Execution Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1803: Parallels Desktop Updater Improper Verification of Cryptographic Signature Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1802: Ivanti Avalanche Printer Device Service Missing Authentication Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1801: Ivanti Avalanche Smart Device Service Missing Authentication Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Tue, 19 Dec 2023

*ZDI-23-1800: Ivanti Avalanche EnterpriseServer Service Unrestricted File Upload Local Privilege Escalation Vulnerability*

- [Link](#)

---

”

## Die Hacks der Woche

mit Martin Haunschmid

Ihr habt WAS in eure Züge programmiert!?



[Zum Youtube Video](#)

## Cyberangriffe: (Dez)

Datum	Opfer	Land	Information
2023-12-20	Kitco	[CAN]	<a href="#">Link</a>
2023-12-19	HCL Technologies	[IND]	<a href="#">Link</a>
2023-12-18	Elektroprivreda Srbije (EPS)	[SRB]	<a href="#">Link</a>
2023-12-17	Socadis	[CAN]	<a href="#">Link</a>
2023-12-14	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
2023-12-22	[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>
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	[dbmgroup.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>



Datum	Opfer	Ransomware-Gruppe	Webseite
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.copreintacional.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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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	[berkshireesupply.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	[navitaspet.com]	blackbasta	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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]	clon	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	[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	[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	[Leedarson 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

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-13	[TglT]	dragonforce	<a href="#">Link</a>
2023-12-13	[Seven Seas]	dragonforce	<a href="#">Link</a>
2023-12-13	[Decina]	dragonforce	<a href="#">Link</a>
2023-12-13	[Cooper Research Technology]	dragonforce	<a href="#">Link</a>
2023-12-13	[Greater Cincinnati Behavioral Health]	dragonforce	<a href="#">Link</a>
2023-12-13	[ccadm.org]	lockbit3	<a href="#">Link</a>
2023-12-13	[dawsongroup.co.uk]	lockbit3	<a href="#">Link</a>
2023-12-13	[altezze.com.mx]	lockbit3	<a href="#">Link</a>
2023-12-13	[Tulane University]	meow	<a href="#">Link</a>
2023-12-13	[thirdstreetbrewhouse.com carolinabeveragegroup.com]	blackbasta	<a href="#">Link</a>
2023-12-13	[Advantage Group International]	alphv	<a href="#">Link</a>
2023-12-13	[Dameron Hospital]	ransomhouse	<a href="#">Link</a>
2023-12-13	[agy.com]	blackbasta	<a href="#">Link</a>
2023-12-13	[alexander-dennis.com]	blackbasta	<a href="#">Link</a>
2023-12-13	[Dillard Door & Security]	cactus	<a href="#">Link</a>
2023-12-13	[cms.law]	lockbit3	<a href="#">Link</a>
2023-12-13	[SBK Real Estate]	8base	<a href="#">Link</a>
2023-12-13	[CACG]	8base	<a href="#">Link</a>
2023-12-13	[VAC-U-MAX]	8base	<a href="#">Link</a>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[Tcman]	rhysida	<a href="#">Link</a>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[ychlcsc.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
2023-12-01	[Hello Cristina from Law Offices of John E Hill]	monti	Link
2023-12-01	[Hello Jacobs from RVC]	monti	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-01	[Austal]	hunters	<a href="#">Link</a>
2023-12-01	[St. Johns River Water Management District]	hunters	<a href="#">Link</a>
2023-12-01	[Kellett & Bartholow PLLC]	incransom	<a href="#">Link</a>
2023-12-01	[Centroedile Milano]	blacksuit	<a href="#">Link</a>
2023-12-01	[Iptor]	akira	<a href="#">Link</a>
2023-12-01	[farwickgrote.de]	cloak	<a href="#">Link</a>
2023-12-01	[skncustoms.com]	cloak	<a href="#">Link</a>
2023-12-01	[euro2000-spa.it]	cloak	<a href="#">Link</a>
2023-12-01	[Thenewtrongroup.com]	cloak	<a href="#">Link</a>
2023-12-01	[Bankofceylon.co.uk]	cloak	<a href="#">Link</a>
2023-12-01	[carranza.on.ca]	cloak	<a href="#">Link</a>
2023-12-01	[Agamatrix]	meow	<a href="#">Link</a>

# 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.