



Ausgabe: 20231127

# 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

### *Synology schließt Pwn2Own-Lücke in Router-Manager-Firmware*

Im Betriebssystem für Synology-Router haben IT-Forscher beim Pwn2Own-Wettbewerb Sicherheitslücken aufgedeckt. Ein Update schließt sie.

- [Link](#)

---

### *Sicherheitsupdates: Foxit PDF unter macOS und Windows verwundbar*

Die Entwickler haben in aktuellen Versionen von Foxit PDF Reader und PDF Editor mehrere Schwachstellen geschlossen.

- [Link](#)

---

### *Cloud-Computing-Software ownCloud und Nextcloud angreifbar*

Angreifer können unbefugt auf Dateien auf Nextcloud- und ownCloud-Servern zugreifen. Sicherheitsupdates und Workarounds schaffen Abhilfe.

- [Link](#)

---

### *Atlassian rüstet Jira Data Center and Server & Co. gegen mögliche Attacken*

Es gibt wichtige Sicherheitsupdates für verschiedene Softwarelösungen von Atlassian. Es kann Schadcode auf Systeme gelangen.

- [Link](#)

---

### *Mozilla erweitert Datenschutz und Sicherheit von Firefox und Thunderbird*

Durch Schwachstellen in Mozillas Mailclient und Webbrowser kann Schadcode schlüpfen. Außerdem wurde der Datenschutz verbessert.

- [Link](#)

---

### *Sicherheitsforscher finden kritische Fehler in KI-Werkzeugen Ray, MLflow und H2O*

Die beliebten Werkzeuge für KI-Anwendungen leiden unter Codeschmuggel, illegitimen Dateimanipulationen und anderen Bugs. Nicht immer sind Updates verfügbar.

- [Link](#)

---

### *Synology schließt kritische Firmware-Lücke in Überwachungskameras*

Angreifer können eigenen Code auf Überwachungskameras von Synology ausführen.

- [Link](#)

---

### *Updates für Trellix ePolicy Orchestrator schließen Sicherheitslücken*

Trellix, Nachfolger von McAfee und FireEye, hat den ePolicy Orchestrator aktualisiert. Das Update schließt etwa eine hochriskant eingestufte Schwachstelle.

- [Link](#)

---

### *Code-Schmuggel: Neue Splunk-Versionen beheben Sicherheitslücken*

Unsichere XML-Verarbeitung und ungenügende Prüfung von Logeinträgen ermöglichten Angreifern, eigenen Code in Splunk-Produkte zu schleusen.

- [Link](#)

---

### *Sicherheitsupdates: Juniper Secure Analytics ist angreifbar*

Angreifer können Lücken in Junipers SIEM-Lösung als Sprungbrett ausnutzen und sich zum Root-Nutzer machen.

- [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-2023-4966	0.922670000	0.987080000	<a href="#">Link</a>
CVE-2023-46747	0.965530000	0.995010000	<a href="#">Link</a>
CVE-2023-46604	0.966470000	0.995360000	<a href="#">Link</a>
CVE-2023-42793	0.972640000	0.998130000	<a href="#">Link</a>
CVE-2023-38035	0.970400000	0.996950000	<a href="#">Link</a>
CVE-2023-35078	0.964440000	0.994570000	<a href="#">Link</a>
CVE-2023-34362	0.928450000	0.987830000	<a href="#">Link</a>
CVE-2023-34039	0.925730000	0.987500000	<a href="#">Link</a>
CVE-2023-33246	0.970860000	0.997170000	<a href="#">Link</a>
CVE-2023-32315	0.957520000	0.992640000	<a href="#">Link</a>
CVE-2023-30625	0.925770000	0.987510000	<a href="#">Link</a>
CVE-2023-30013	0.925700000	0.987490000	<a href="#">Link</a>
CVE-2023-28771	0.918550000	0.986590000	<a href="#">Link</a>
CVE-2023-27372	0.971190000	0.997320000	<a href="#">Link</a>
CVE-2023-27350	0.971980000	0.997750000	<a href="#">Link</a>
CVE-2023-26469	0.915280000	0.986200000	<a href="#">Link</a>
CVE-2023-26360	0.913940000	0.986060000	<a href="#">Link</a>
CVE-2023-25717	0.962680000	0.993930000	<a href="#">Link</a>
CVE-2023-25194	0.910980000	0.985730000	<a href="#">Link</a>
CVE-2023-2479	0.958820000	0.992960000	<a href="#">Link</a>
CVE-2023-24489	0.969450000	0.996580000	<a href="#">Link</a>
CVE-2023-22518	0.967630000	0.995850000	<a href="#">Link</a>
CVE-2023-22515	0.955290000	0.992100000	<a href="#">Link</a>
CVE-2023-21839	0.956630000	0.992430000	<a href="#">Link</a>
CVE-2023-21823	0.955130000	0.992050000	<a href="#">Link</a>
CVE-2023-21554	0.961220000	0.993540000	<a href="#">Link</a>
CVE-2023-20887	0.950720000	0.991160000	<a href="#">Link</a>
CVE-2023-1671	0.952600000	0.991530000	<a href="#">Link</a>
CVE-2023-0669	0.966380000	0.995320000	<a href="#">Link</a>

---

## BSI - Warn- und Informationsdienst (WID)

Fri, 24 Nov 2023

*[UPDATE] [hoch] Atlassian Bamboo, Atlassian Bitbucket, Atlassian Confluence and Atlassian Jira Software: Mehrere Schwachstellen*

Ein Angreifer kann mehrere Schwachstellen in Atlassian Bamboo, Atlassian Bitbucket, Atlassian Confluence und Atlassian Jira Software ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

---

Fri, 24 Nov 2023

**[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen**

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

- [Link](#)

---

Fri, 24 Nov 2023

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

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

---

Fri, 24 Nov 2023

**[UPDATE] [hoch] Intel Prozessoren: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Intel Prozessoren ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern oder Informationen offenzulegen.

- [Link](#)

---

Fri, 24 Nov 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, 23 Nov 2023

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel und Oracle Linux ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Thu, 23 Nov 2023

**[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

---

Thu, 23 Nov 2023

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

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

- [Link](#)

---

Thu, 23 Nov 2023

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

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

- [Link](#)

---

Thu, 23 Nov 2023

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

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

- [Link](#)

---

Thu, 23 Nov 2023

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

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

- [Link](#)

---

Thu, 23 Nov 2023

**[UPDATE] [hoch] Mozilla Firefox und 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, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

- [Link](#)

---

Thu, 23 Nov 2023

**[UPDATE] [hoch] Microsoft Entwicklerwerkzeuge: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft ASP.NET, Microsoft Visual Studio und Microsoft Visual Studio Code ausnutzen, um Sicherheitsmechanismen zu umgehen, um seine Privilegien zu erhöhen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Thu, 23 Nov 2023

**[UPDATE] [hoch] strongSwan: Schwachstelle ermöglicht Codeausführung und DoS**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in strongSwan ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

---

Thu, 23 Nov 2023

**[NEU] [hoch] IGEL OS: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in IGEL OS ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service zu verursachen.

- [Link](#)

---

Wed, 22 Nov 2023

**[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen**

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

- [Link](#)

---

Wed, 22 Nov 2023

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

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen oder Dateien zu manipulieren.

- [Link](#)

---

Wed, 22 Nov 2023

**[NEU] [UNGEPATCHT] [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](#)

---

Wed, 22 Nov 2023

**[NEU] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Erlangung erweiterter Privilegien**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um erweiterte Privilegien zu erlangen.

- [Link](#)

—  
Wed, 22 Nov 2023

**[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen**

Ein entfernter, anonym, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Developer Tools ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)  
—

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/26/2023	[Debian DSA-5565-1 : gst-plugins-bad1.0 - security update]	critical
11/26/2023	[GLSA-202311-16 : Open vSwitch: Multiple Vulnerabilities]	critical
11/25/2023	[SUSE SLES12 Security Update : poppler (SUSE-SU-2023:4546-1)]	critical
11/25/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2023:4551-1)]	critical
11/25/2023	[GLSA-202311-12 : MiniDLNA: Multiple Vulnerabilities]	critical
11/25/2023	[GLSA-202311-10 : RenderDoc: Multiple Vulnerabilities]	critical
11/25/2023	[Fedora 38 : thunderbird (2023-bb021a4854)]	critical
11/24/2023	[Oracle Linux 8 : dotnet6.0 (ELSA-2023-7258)]	critical
11/26/2023	[GLSA-202311-15 : LibreOffice: Multiple Vulnerabilities]	high
11/26/2023	[GLSA-202311-17 : phpMyAdmin: Multiple Vulnerabilities]	high
11/26/2023	[Debian DLA-3666-1 : reportbug - LTS update]	high
11/25/2023	[SUSE SLES15 / openSUSE 15 Security Update : squid (SUSE-SU-2023:4544-1)]	high
11/25/2023	[SUSE SLES12 Security Update : vim (SUSE-SU-2023:4560-1)]	high
11/25/2023	[SUSE SLES12 Security Update : xerces-c (SUSE-SU-2023:4543-1)]	high
11/25/2023	[SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2023:4559-1)]	high
11/25/2023	[SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2023:4558-1)]	high
11/25/2023	[SUSE SLES15 Security Update : slurm_23_02 (SUSE-SU-2023:4565-1)]	high
11/25/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : poppler (SUSE-SU-2023:4562-1)]	high
11/25/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : vim (SUSE-SU-2023:4557-1)]	high
11/25/2023	[SUSE SLES15 / openSUSE 15 Security Update : slurm_23_02 (SUSE-SU-2023:4566-1)]	high
11/25/2023	[SUSE SLES15 Security Update : slurm_23_02 (SUSE-SU-2023:4564-1)]	high
11/25/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : webkit2gtk3 (SUSE-SU-2023:4561-1)]	high
11/25/2023	[SUSE SLES12 Security Update : slurm_23_02 (SUSE-SU-2023:4563-1)]	high
11/25/2023	[SUSE SLES12 Security Update : squid (SUSE-SU-2023:4545-1)]	high
11/25/2023	[Debian DSA-5564-1 : gimp - security update]	high
11/25/2023	[GLSA-202311-14 : GRUB: Multiple Vulnerabilities]	high
11/25/2023	[GLSA-202311-13 : Apptainer: Privilege Escalation]	high
11/25/2023	[GLSA-202311-11 : QtWebEngine: Multiple Vulnerabilities]	high
11/25/2023	[Fedora 37 : golang (2023-7e185b8c12)]	high
11/25/2023	[Fedora 38 : chromium (2023-5b46676afa)]	high
11/25/2023	[Fedora 38 : webkitgtk (2023-11aaf99627)]	high
11/25/2023	[Debian DLA-3665-1 : node-json5 - LTS security update]	high
11/25/2023	[Debian DLA-3662-1 : freeimage - LTS security update]	high

Datum	Schwachstelle	Bewertung
11/24/2023	[GLSA-202311-05 : LinuxCIFS utils: Multiple Vulnerabilities]	high
11/24/2023	[FreeBSD : strongSwan – vulnerability in charon-tkm (a62c0c50-8aa0-11ee-ac0d-00e0670f2660)]	high
11/24/2023	[Debian DLA-3663-1 : strongswan - LTS security update]	high
11/24/2023	[Fedora 37 : kubernetes (2023-6ad09ef90b)]	high



# Aktiv ausgenutzte Sicherheitslücken

## Exploits der letzten 5 Tage

“Sat, 25 Nov 2023

### ***CE Phoenix 1.0.8.20 Cross Site Scripting***

CE Phoenix version 1.0.8.20 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

---

” “Sat, 25 Nov 2023

### ***PyroCMS 3.0.1 Cross Site Scripting***

PyroCMS version 3.0.1 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

---

” “Sat, 25 Nov 2023

### ***CSZ CMS 1.3.0 Shell Upload***

CSZ CMS version 1.3.0 suffers from a remote shell upload vulnerability.

- [Link](#)

---

” “Wed, 22 Nov 2023

### ***WordPress UserPro 5.1.x Password Reset / Authentication Bypass / Escalation***

WordPress UserPro plugin versions 5.1.1 and below suffer from an insecure password reset mechanism, information disclosure, and authentication bypass vulnerabilities. Versions 5.1.4 and below suffer from privilege escalation and shortcode execution vulnerabilities.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***Magento 2.4.6 XSLT Server Side Injection***

Magento version 2.4.6 XSLT server-side injection proof of concept exploit.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***PHPJabbers Availability Booking Calendar 5.0 Cross Site Scripting***

PHPJabbers Availability Booking Calendar version 5.0 suffers from multiple cross site scripting vulnerabilities.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***PHPJabbers Availability Booking Calendar 5.0 CSV Injection***

PHPJabbers Availability Booking Calendar version 5.0 suffers from a CSV injection vulnerability.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***GaatiTrack Courier Management System 1.0 Cross Site Scripting***

GaatiTrack Courier Management System version 1.0 suffers from multiple cross site scripting vulnerabilities.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***Jorani Leave Management System 1.0.2 Host Header Injection***

Jorani Leave Management System version 1.0.2 suffers from a host header injection vulnerability.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***FireBear Improved Import And Export 3.8.6 XSLT Server Side Injection***

FireBear Improved Import and Export version 3.8.6 for Magento 2.4.6 suffers from an XSLT server-side injection vulnerability that allows for command execution.

- [Link](#)

---

” “Mon, 20 Nov 2023

### ***Shuttle Booking Software 2.0 Cross Site Scripting***

Shuttle Booking Software version 2.0 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

---

” “Fri, 17 Nov 2023

***Magento 2.4.6 XSLT Server Side Injection / Command Execution***

Magento version 2.4.6 suffers from an XSLT server side injection vulnerability that allows for remote command execution.

- [Link](#)

---

” “Wed, 15 Nov 2023

***EzViz Studio 2.2.0 DLL Hijacking***

EzViz Studio version 2.2.0 suffers from a dll hijacking vulnerability.

- [Link](#)

---

” “Tue, 14 Nov 2023

***EnBw SENEK Legacy Storage Box Log Disclosure***

EnBw SENEK Legacy Storage Box versions 1 through 3 suffer from a log disclosure vulnerability.

- [Link](#)

---

” “Tue, 14 Nov 2023

***AjaxPro Deserialization Remote Code Execution***

This Metasploit module leverages an insecure deserialization of data to get remote code execution on the target OS in the context of the user running the website which utilized AjaxPro. To achieve code execution, the module will construct some JSON data which will be sent to the target. This data will be deserialized by the AjaxPro JsonSerializer and will trigger the execution of the payload. All AjaxPro versions prior to 21.10.30.1 are vulnerable to this issue, and a vulnerable method which can be used to trigger the deserialization exists in the default AjaxPro namespace. AjaxPro 21.10.30.1 removed the vulnerable method, but if a custom method that accepts a parameter of type that is assignable from ObjectDataProvider (e.g. object) exists, the vulnerability can still be exploited. This module has been tested successfully against official AjaxPro on version 7.7.31.1 without any modification, and on version 21.10.30.1 with a custom vulnerable method added.

- [Link](#)

---

” “Tue, 14 Nov 2023

***Apache ActiveMQ Unauthenticated Remote Code Execution***

This Metasploit module exploits a deserialization vulnerability in the OpenWire transport unmarshaller in Apache ActiveMQ. Affected versions include 5.18.0 through to 5.18.2, 5.17.0 through to 5.17.5, 5.16.0 through to 5.16.6, and all versions before 5.15.16.

- [Link](#)

---

” “Tue, 14 Nov 2023

***ZoneMinder Snapshots Command Injection***

This Metasploit module exploits an unauthenticated command injection in zoneminder that can be exploited by appending a command to an action of the snapshot view. Versions prior to 1.36.33 and 1.37.33 are affected.

- [Link](#)

---

” “Tue, 14 Nov 2023

***Cisco IOX XE Unauthenticated Remote Code Execution***

This Metasploit module leverages both CVE-2023-20198 and CVE-2023-20273 against vulnerable instances of Cisco IOS XE devices which have the web UI exposed. An attacker can execute a payload with root privileges. The vulnerable IOS XE versions are 16.1.1, 16.1.2, 16.1.3, 16.2.1, 16.2.2, 16.3.1, 16.3.2, 16.3.3, 16.3.1a, 16.3.4, 16.3.5, 16.3.5b, 16.3.6, 16.3.7, 16.3.8, 16.3.9, 16.3.10, 16.3.11, 16.4.1, 16.4.2, 16.4.3, 16.5.1, 16.5.1a, 16.5.1b, 16.5.2, 16.5.3, 16.6.1, 16.6.2, 16.6.3, 16.6.4, 16.6.5, 16.6.4s, 16.6.4a, 16.6.5a, 16.6.6, 16.6.5b, 16.6.7, 16.6.7a, 16.6.8, 16.6.9, 16.6.10, 16.7.1, 16.7.1a, 16.7.1b, 16.7.2, 16.7.3, 16.7.4, 16.8.1, 16.8.1a, 16.8.1b, 16.8.1s, 16.8.1c, 16.8.1d, 16.8.2, 16.8.1e, 16.8.3, 16.9.1, 16.9.2, 16.9.1a, 16.9.1b, 16.9.1s, 16.9.1c, 16.9.1d, 16.9.3, 16.9.2a, 16.9.2s, 16.9.3h, 16.9.4, 16.9.3s, 16.9.3a, 16.9.4c, 16.9.5, 16.9.5f, 16.9.6, 16.9.7, 16.9.8, 16.9.8a, 16.9.8b, 16.9.8c, 16.10.1, 16.10.1a, 16.10.1b, 16.10.1s, 16.10.1c, 16.10.1e, 16.10.1d, 16.10.2, 16.10.1f, 16.10.1g, 16.10.3, 16.11.1, 16.11.1a, 16.11.1b, 16.11.2, 16.11.1s, 16.11.1c, 16.12.1, 16.12.1s, 16.12.1a, 16.12.1c, 16.12.1w, 16.12.2, 16.12.1y, 16.12.2a, 16.12.3, 16.12.8, 16.12.2s, 16.12.1x, 16.12.1t, 16.12.2t, 16.12.4, 16.12.3s, 16.12.1z, 16.12.3a, 16.12.4a, 16.12.5, 16.12.6, 16.12.1z1, 16.12.5a, 16.12.5b, 16.12.1z2, 16.12.6a, 16.12.7, 16.12.9, 16.12.10, 17.1.1, 17.1.1a, 17.1.1s, 17.1.2, 17.1.1t, 17.1.3, 17.2.1, 17.2.1r, 17.2.1a, 17.2.1v, 17.2.2, 17.2.3, 17.3.1, 17.3.2, 17.3.3, 17.3.1a, 17.3.1w, 17.3.2a, 17.3.1x, 17.3.1z, 17.3.3a, 17.3.4, 17.3.5, 17.3.4a, 17.3.6, 17.3.4b, 17.3.4c, 17.3.5a, 17.3.5b, 17.3.7, 17.3.8, 17.4.1, 17.4.2, 17.4.1a, 17.4.1b, 17.4.1c, 17.4.2a, 17.5.1, 17.5.1a, 17.5.1b, 17.5.1c, 17.6.1, 17.6.2, 17.6.1w, 17.6.1a, 17.6.1x, 17.6.3, 17.6.1y, 17.6.1z, 17.6.3a, 17.6.4, 17.6.1z1, 17.6.5, 17.6.6, 17.7.1, 17.7.1a, 17.7.1b, 17.7.2, 17.10.1,

17.10.1a, 17.10.1b, 17.8.1, 17.8.1a, 17.9.1, 17.9.1w, 17.9.2, 17.9.1a, 17.9.1x, 17.9.1y, 17.9.3, 17.9.2a, 17.9.1x1, 17.9.3a, 17.9.4, 17.9.1y1, 17.11.1, 17.11.1a, 17.12.1, 17.12.1a, and 17.11.99SW.

- [Link](#)

---

” “Tue, 14 Nov 2023

***F5 BIG-IP TMUI AJP Smuggling Remote Command Execution***

This Metasploit module exploits a flaw in F5's BIG-IP Traffic Management User Interface (TMUI) that enables an external, unauthenticated attacker to create an administrative user. Once the user is created, the module uses the new account to execute a command payload. Both the exploit and check methods automatically delete any temporary accounts that are created.

- [Link](#)

---

” “Tue, 14 Nov 2023

***MagnusBilling Remote Command Execution***

This Metasploit module exploits a command injection vulnerability in MagnusBilling application versions 6.x and 7.x that allows remote attackers to run arbitrary commands via an unauthenticated HTTP request. A piece of demonstration code is present in lib/icepay/icepay.php, with a call to an exec(). The parameter to exec() includes the GET parameter democ, which is controlled by the user and not properly sanitised/escaped. After successful exploitation, an unauthenticated user is able to execute arbitrary OS commands. The commands run with the privileges of the web server process, typically www-data or asterisk. At a minimum, this allows an attacker to compromise the billing system and its database.

- [Link](#)

---

” “Tue, 14 Nov 2023

***F5 BIG-IP TMUI Directory Traversal / File Upload / Code Execution***

This Metasploit module exploits a directory traversal in F5's BIG-IP Traffic Management User Interface (TMUI) to upload a shell script and execute it as the Unix root user. Unix shell access is obtained by escaping the restricted Traffic Management Shell (TMSH). The escape may not be reliable, and you may have to run the exploit multiple times. Versions 11.6.1-11.6.5, 12.1.0-12.1.5, 13.1.0-13.1.3, 14.1.0-14.1.2, 15.0.0, and 15.1.0 are known to be vulnerable. Fixes were introduced in 11.6.5.2, 12.1.5.2, 13.1.3.4, 14.1.2.6, and 15.1.0.4. Tested against the VMware OVA release of 14.1.2.

- [Link](#)

---

” “Tue, 14 Nov 2023

***mtk-jpeg Driver Out-Of-Bounds Read / Write***

An out-of-bounds read / write due to missing bounds check in the mtk-jpeg driver can lead to memory corruption and potential escalation of privileges.

- [Link](#)

---

” “Tue, 14 Nov 2023

***Android mtk\_jpeg Driver Race Condition / Privilege Escalation***

A race condition in the Android mtk\_jpeg driver can lead to memory corruption and potential local privilege escalation.

- [Link](#)

---

” “Mon, 13 Nov 2023

***Maxima Max Pro Power 1.0 486A BLE Traffic Replay***

Maxima Max Pro Power with firmware version 1.0 486A suffers from a BLE traffic replay vulnerability that allows for arbitrary unauthorized actions.

- [Link](#)

---

” “Mon, 13 Nov 2023

***Windows Kernel Containerized Registry Escape***

The Microsoft Windows kernel suffers from a containerized registry escape through integer overflows in Vrp-BuildKeyPath and other weaknesses.

- [Link](#)

---

”

0-Days der letzten 5 Tage

# Die Hacks der Woche

mit Martin Haunschmid

Eine Zeitreise in die Anfänge des hack-for-hire



[Zum Youtube Video](#)

## Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2023-11-25	HSE (Holding Slovenske Elektranre)	[SVN]	<a href="#">Link</a>
2023-11-25	AVU (Energieversorger)	[DEU]	<a href="#">Link</a>
2023-11-24	UT Health East Texas	[USA]	<a href="#">Link</a>
2023-11-23	Zweckverband gemeindliche Datenverarbeitung im Kreis Neu-Ulm	[DEU]	<a href="#">Link</a>
2023-11-23	Hillcrest HealthCare System	[USA]	<a href="#">Link</a>
2023-11-22	Véligo Location	[FRA]	<a href="#">Link</a>
2023-11-22	Gemeinde Zollikofen	[CHE]	<a href="#">Link</a>
2023-11-22	Svenska kyrkan (l'Église suédoise)	[SWE]	<a href="#">Link</a>
2023-11-19	Rostocker Straßenbahn AG (RSAG)	[DEU]	<a href="#">Link</a>
2023-11-18	Fidelity National Financial (FNF)	[USA]	<a href="#">Link</a>
2023-11-17	SIAAP (Syndicat Interdépartemental pour l'Assainissement de l'Agglomération Parisienne)	[FRA]	<a href="#">Link</a>
2023-11-17	Mössinger Stadtverwaltung	[DEU]	<a href="#">Link</a>
2023-11-16	Etelä-Savon ammattiopisto Esedu	[FIN]	<a href="#">Link</a>
2023-11-16	Sabre Insurance Group	[GBR]	<a href="#">Link</a>
2023-11-15	Meredosia-Chambersburg school district	[USA]	<a href="#">Link</a>
2023-11-14	Bladen County Government	[USA]	<a href="#">Link</a>
2023-11-14	North Muskegon Public Schools	[USA]	<a href="#">Link</a>
2023-11-14	Beaverton School District	[USA]	<a href="#">Link</a>
2023-11-14	City of Long Beach	[USA]	<a href="#">Link</a>
2023-11-13	Yanfeng	[CHN]	<a href="#">Link</a>
2023-11-13	North Carolina Central University (NCCU)	[USA]	<a href="#">Link</a>
2023-11-12	Huber Heights	[USA]	<a href="#">Link</a>
2023-11-12	Tunstall	[NLD]	<a href="#">Link</a>
2023-11-12	Deutsche Energie-Agentur (Dena)	[DEU]	<a href="#">Link</a>
2023-11-11	Okada Manila	[PHL]	<a href="#">Link</a>
2023-11-10	DP World Australia	[AUS]	<a href="#">Link</a>
2023-11-10	Derichebourg Multiservices	[FRA]	<a href="#">Link</a>
2023-11-10	Glendale Community College (GCC)	[USA]	<a href="#">Link</a>
2023-11-09	Industrial and Commercial Bank of China (ICBC)	[CHN]	<a href="#">Link</a>
2023-11-09	Tri-City Medical Center	[USA]	<a href="#">Link</a>
2023-11-09	Henry County Schools	[USA]	<a href="#">Link</a>
2023-11-08	York Region District School Board	[CAN]	<a href="#">Link</a>
2023-11-08	Hellenic Public Properties Company (ETAD)	[GRC]	<a href="#">Link</a>
2023-11-07	Comhairle nan Eilean Siar	[GBR]	<a href="#">Link</a>
2023-11-07	Harris Center for Mental Health and IDD	[USA]	<a href="#">Link</a>
2023-11-07	Washington State Department of Transportation (WSDOT)	[USA]	<a href="#">Link</a>
2023-11-06	KaDeWe	[DEU]	<a href="#">Link</a>
2023-11-05	Le conseil départemental du Loiret	[FRA]	<a href="#">Link</a>
2023-11-05	Madison Memorial Hospital	[USA]	<a href="#">Link</a>
2023-11-05	Pulaski County Public Schools (PCPS)	[USA]	<a href="#">Link</a>
2023-11-05	Concevis AG	[CHE]	<a href="#">Link</a>
2023-11-04	Butte School District	[USA]	<a href="#">Link</a>
2023-11-02	Infosys McCamish Systems	[USA]	<a href="#">Link</a>
2023-11-02	Crystal Run Healthcare	[USA]	<a href="#">Link</a>
2023-11-01	Mr. Cooper Group	[USA]	<a href="#">Link</a>
2023-11-01	Rekord Fenster Türen	[DEU]	<a href="#">Link</a>
2023-11-01	EDC	[DNK]	<a href="#">Link</a>
2023-11-01	Cogdell Memorial Hospital	[USA]	<a href="#">Link</a>

## Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-26	[Katsky Korins]	meow	<a href="#">Link</a>
2023-11-26	[AlJaber Engineering]	ransomexx	<a href="#">Link</a>
2023-11-26	[ALAB laboratoria ]	ragroup	<a href="#">Link</a>
2023-11-25	[kenso.com.my]	lockbit3	<a href="#">Link</a>
2023-11-25	[SWISHSMILES.COM]	clop	<a href="#">Link</a>
2023-11-25	[TXWES.EDU]	clop	<a href="#">Link</a>
2023-11-25	[SWEETLAKE.COM]	clop	<a href="#">Link</a>
2023-11-25	[SGMGROUP.COM]	clop	<a href="#">Link</a>
2023-11-25	[MORSKATEMANUFACTURING.COM]	clop	<a href="#">Link</a>
2023-11-24	[Hampton Newport News CSB (Last chance)]	alphv	<a href="#">Link</a>
2023-11-24	[Energy China]	rhysida	<a href="#">Link</a>
2023-11-18	[TALENTUM Temporal SAS]	noescape	<a href="#">Link</a>
2023-11-24	[carriereindustrial.com]	donutleaks	<a href="#">Link</a>
2023-11-24	[Albert, Righter & Tittmann architechts, inc.]	donutleaks	<a href="#">Link</a>
2023-11-24	[nrtw.org]	lockbit3	<a href="#">Link</a>
2023-11-24	[preidlhof.it]	lockbit3	<a href="#">Link</a>
2023-11-24	[ribolia.com]	lockbit3	<a href="#">Link</a>
2023-11-24	[Lincoln Office]	hunters	<a href="#">Link</a>
2023-11-24	[LCA Consultores]	alphv	<a href="#">Link</a>
2023-11-24	[TJM PRODUCTS PTY. LTD]	alphv	<a href="#">Link</a>
2023-11-24	[Spectrum Solutions LLC]	alphv	<a href="#">Link</a>
2023-11-05	[Es Saadi]	meow	<a href="#">Link</a>
2023-11-05	[Zenithpharma]	meow	<a href="#">Link</a>
2023-11-05	[Back Roads]	meow	<a href="#">Link</a>
2023-11-09	[Equaldex]	meow	<a href="#">Link</a>
2023-11-18	[Vanderbilt University Medical Center]	meow	<a href="#">Link</a>
2023-11-22	[Standard Filter]	meow	<a href="#">Link</a>
2023-11-23	[des-ae.com]	lockbit3	<a href="#">Link</a>
2023-11-23	[unidesign-jewel.com]	lockbit3	<a href="#">Link</a>
2023-11-23	[Eckell Sparks Law Firm]	alphv	<a href="#">Link</a>
2023-11-23	[officinaverdedesign.it]	lockbit3	<a href="#">Link</a>
2023-11-23	[B+P Gerüstbau GmbH]	incransom	<a href="#">Link</a>
2023-11-23	[DM Civil Co.]	incransom	<a href="#">Link</a>
2023-11-23	[Ingo Money Inc]	incransom	<a href="#">Link</a>
2023-11-23	[Nicole Miller]	incransom	<a href="#">Link</a>
2023-11-23	[Pro Metals LLC]	incransom	<a href="#">Link</a>
2023-11-23	[Springfield Area Chamber of Commerce]	incransom	<a href="#">Link</a>
2023-11-23	[Trylon TSF Inc.]	incransom	<a href="#">Link</a>
2023-11-22	[McHale Landscape Design]	play	<a href="#">Link</a>
2023-11-22	[Fidelity National Financial]	alphv	<a href="#">Link</a>
2023-11-22	[Alspec]	akira	<a href="#">Link</a>
2023-11-22	[Custom Engineering &Fabrication, Inc.]	akira	<a href="#">Link</a>
2023-11-22	[IQ Supply Solutions]	akira	<a href="#">Link</a>
2023-11-22	[NESPOLI GROUP]	alphv	<a href="#">Link</a>
2023-11-22	[Community Hospital]	medusa	<a href="#">Link</a>
2023-11-22	[merz-elektro.de]	lockbit3	<a href="#">Link</a>
2023-11-22	[art-eco.it]	lockbit3	<a href="#">Link</a>
2023-11-22	[therobisongroup.com]	lockbit3	<a href="#">Link</a>
2023-11-22	[ds-granit.fr]	threeam	<a href="#">Link</a>
2023-11-21	[APVL ingénierie]	8base	<a href="#">Link</a>
2023-11-21	[Cold Car Spa]	8base	<a href="#">Link</a>
2023-11-21	[La Contabile Spa]	8base	<a href="#">Link</a>
2023-11-21	[DMC Luxembourg]	8base	<a href="#">Link</a>
2023-11-22	[Hills Legal Group Ltd]	8base	<a href="#">Link</a>
2023-11-22	[Brown's Bay Packing Company]	8base	<a href="#">Link</a>
2023-11-22	[Hahn and Clay, Inc.]	8base	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-22	[Imperiali AG]	8base	<a href="#">Link</a>
2023-11-21	[[DATA] Bakrie Group & Bakrie Sumatera Plantations]	alphv	<a href="#">Link</a>
2023-11-21	[floydskerenlaw.com]	lockbit3	<a href="#">Link</a>
2023-11-21	[bnpmmedia.com]	lockbit3	<a href="#">Link</a>
2023-11-21	[Verhelst]	cactus	<a href="#">Link</a>
2023-11-21	[Petersen Health Care]	cactus	<a href="#">Link</a>
2023-11-21	[Paul Stuart]	cactus	<a href="#">Link</a>
2023-11-21	[Crystal Lake Health Center]	hunters	<a href="#">Link</a>
2023-11-21	[qautomotive.com.au]	lockbit3	<a href="#">Link</a>
2023-11-21	[martinique.no]	lockbit3	<a href="#">Link</a>
2023-11-21	[phihydraulics.com]	lockbit3	<a href="#">Link</a>
2023-11-21	[St Edmund's College & Prep School]	rhysida	<a href="#">Link</a>
2023-11-21	[helifrusa.com]	lockbit3	<a href="#">Link</a>
2023-11-21	[Bolidt]	bianlian	<a href="#">Link</a>
2023-11-21	[Growers Express]	bianlian	<a href="#">Link</a>
2023-11-21	[NSEIT Limited (a subsidiary of the National Stock Exchange of India)]	bianlian	<a href="#">Link</a>
2023-11-11	[Rc Moore Inc]	noescape	<a href="#">Link</a>
2023-11-10	[Enware Australia Pty Ltd]	noescape	<a href="#">Link</a>
2023-11-20	[sabre.co.uk]	lockbit3	<a href="#">Link</a>
2023-11-20	[nybravestfcu.org]	lockbit3	<a href="#">Link</a>
2023-11-20	[Hampton Newport News CSB]	alphv	<a href="#">Link</a>
2023-11-20	[jlgmarine.com]	blackbasta	<a href="#">Link</a>
2023-11-12	[Studio D.EL.LA. SRL]	knight	<a href="#">Link</a>
2023-11-14	[Barnett Millworks]	knight	<a href="#">Link</a>
2023-11-20	[Dreyfuss Williams & Associates Co., LPA]	knight	<a href="#">Link</a>
2023-11-20	[onyourmark.org]	lockbit3	<a href="#">Link</a>
2023-11-20	[agrovi.dk]	blackbasta	<a href="#">Link</a>
2023-11-20	[arenaproducts.com]	blackbasta	<a href="#">Link</a>
2023-11-20	[etude-villa.fr]	blackbasta	<a href="#">Link</a>
2023-11-16	[UPDATE! FEAM Maintenance]	alphv	<a href="#">Link</a>
2023-11-20	[brownintegratedlogistics.com]	lockbit3	<a href="#">Link</a>
2023-11-20	[British Library]	rhysida	<a href="#">Link</a>
2023-11-22	[Hahn & Clay, Inc.]	8base	<a href="#">Link</a>
2023-11-19	[Tackle West]	alphv	<a href="#">Link</a>
2023-11-19	[U.L. COLEMAN COMPANIES]	alphv	<a href="#">Link</a>
2023-11-19	[Autonomous Flight - @autonomousfly]	alphv	<a href="#">Link</a>
2023-11-18	[The DMC]	play	<a href="#">Link</a>
2023-11-18	[nealbrothers.co.uk]	threeam	<a href="#">Link</a>
2023-11-18	[generalrefrig.com]	lockbit3	<a href="#">Link</a>
2023-11-17	[PruittHealth]	noescape	<a href="#">Link</a>
2023-11-17	[ajcfood.com]	lockbit3	<a href="#">Link</a>
2023-11-17	[CENTRE D'AUTO P.R.N. SALABERRY IN]	medusa	<a href="#">Link</a>
2023-11-17	[McCray & Withrow ]	medusa	<a href="#">Link</a>
2023-11-17	[Metro MPLS]	akira	<a href="#">Link</a>
2023-11-17	[HAESUNG DS CO Ltd]	qilin	<a href="#">Link</a>
2023-11-05	[Kwik Industries, Inc.]	noescape	<a href="#">Link</a>
2023-11-17	[WellLife Network Inc.]	incransom	<a href="#">Link</a>
2023-11-17	[ATC SA]	akira	<a href="#">Link</a>
2023-11-17	[Select Education Group]	blacksuit	<a href="#">Link</a>
2023-11-17	[edc.dk]	blackbasta	<a href="#">Link</a>
2023-11-17	[villanuevadelaserena.es]	lockbit3	<a href="#">Link</a>
2023-11-17	[Admilla ELAP]	ransomexx	<a href="#">Link</a>
2023-11-17	[Aceromex ]	ragroup	<a href="#">Link</a>
2023-11-17	[Chung Hwa Chemical Industrial Works ]	ragroup	<a href="#">Link</a>
2023-11-17	[SUMMIT VETERINARY PHARMACEUTICALS LIMITED ]	ragroup	<a href="#">Link</a>
2023-11-17	[Informist Media ]	ragroup	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-17	[Epstein Law]	qilin	<a href="#">Link</a>
2023-11-16	[Toyota Financial]	medusa	<a href="#">Link</a>
2023-11-17	[owensgroup.uk]	lockbit3	<a href="#">Link</a>
2023-11-17	[hsksgreenhalgh.co.uk]	lockbit3	<a href="#">Link</a>
2023-11-17	[krblaw.com]	lockbit3	<a href="#">Link</a>
2023-11-17	[communitydentalme.org]	lockbit3	<a href="#">Link</a>
2023-11-17	[chicagotrading.com]	lockbit3	<a href="#">Link</a>
2023-11-17	[adyne.com]	lockbit3	<a href="#">Link</a>
2023-11-17	[goodhopeholdings.com]	lockbit3	<a href="#">Link</a>
2023-11-17	[planethomelending.com]	lockbit3	<a href="#">Link</a>
2023-11-15	[Decatur Independent School District]	incransom	<a href="#">Link</a>
2023-11-16	[Consilium staffing llc]	incransom	<a href="#">Link</a>
2023-11-15	[Yamaha Motor Philippines,Inc.]	incransom	<a href="#">Link</a>
2023-11-15	[Guardian Alarm]	incransom	<a href="#">Link</a>
2023-11-15	[SCOLARI Srl]	incransom	<a href="#">Link</a>
2023-11-16	[uchlogistics.co.uk]	blackbasta	<a href="#">Link</a>
2023-11-16	[citycontainer.dk]	blackbasta	<a href="#">Link</a>
2023-11-16	[FEAM Maintenance]	alphv	<a href="#">Link</a>
2023-11-16	[thewalkerschool]	alphv	<a href="#">Link</a>
2023-11-15	[MeridianLink fails to file with the SEC..so we do it for them + 24 hours to pay]	alphv	<a href="#">Link</a>
2023-11-15	[EOS]	lorenz	<a href="#">Link</a>
2023-11-15	[THK Co., Ltd.]	hunters	<a href="#">Link</a>
2023-11-15	[Cardinal MetalWorks]	alphv	<a href="#">Link</a>
2023-11-15	[ADH Health Products Inc]	alphv	<a href="#">Link</a>
2023-11-08	[Ingeniería FULCRUM]	8base	<a href="#">Link</a>
2023-11-09	[Scheidt GmbH]	8base	<a href="#">Link</a>
2023-11-15	[Gallagher Tire, Inc.]	8base	<a href="#">Link</a>
2023-11-15	[MODERNGRAB, S.A.]	8base	<a href="#">Link</a>
2023-11-15	[Storey Trucking Company, Inc.]	8base	<a href="#">Link</a>
2023-11-15	[APREVYA]	8base	<a href="#">Link</a>
2023-11-15	[Lanificio Luigi Colombo S.p.A.]	8base	<a href="#">Link</a>
2023-11-15	[MERRILL Technologies Group]	8base	<a href="#">Link</a>
2023-11-15	[Ontario Pork]	8base	<a href="#">Link</a>
2023-11-15	[Parsons Investments]	8base	<a href="#">Link</a>
2023-11-15	[kwhfreeze.fi]	lockbit3	<a href="#">Link</a>
2023-11-14	[PIKE Technologies]	play	<a href="#">Link</a>
2023-11-14	[Proforma Albrecht]	play	<a href="#">Link</a>
2023-11-14	[Fgs]	play	<a href="#">Link</a>
2023-11-14	[Trademark Property]	play	<a href="#">Link</a>
2023-11-14	[Nomot]	play	<a href="#">Link</a>
2023-11-14	[Global Technologies Racing Ltd]	play	<a href="#">Link</a>
2023-11-14	[Thompson Candy]	play	<a href="#">Link</a>
2023-11-14	[Road Scholar Transport]	play	<a href="#">Link</a>
2023-11-14	[KaDeWe]	play	<a href="#">Link</a>
2023-11-14	[Wyatt Detention Center]	play	<a href="#">Link</a>
2023-11-14	[Guntert & Zimmerman]	play	<a href="#">Link</a>
2023-11-14	[ConSpare]	play	<a href="#">Link</a>
2023-11-14	[Premise Health]	alphv	<a href="#">Link</a>
2023-11-15	[MeridianLink]	alphv	<a href="#">Link</a>
2023-11-14	[Gnome Landscapes]	alphv	<a href="#">Link</a>
2023-11-14	[agromatic.de]	blackbasta	<a href="#">Link</a>
2023-11-14	[cmcsheetmetal.com]	blackbasta	<a href="#">Link</a>
2023-11-14	[rekord.de]	blackbasta	<a href="#">Link</a>
2023-11-14	[boulangerieauger.com]	blackbasta	<a href="#">Link</a>
2023-11-14	[maytec.de]	blackbasta	<a href="#">Link</a>
2023-11-14	[SheelaFoam]	alphv	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-14	[Naftor and Grupa Pern (Naftoport/ SIARKOPOL/ SARMATIA/ NAFTOSERWIS) is the most dangerous ]	alphv	<a href="#">Link</a>
2023-11-14	[4set.es]	alphv	<a href="#">Link</a>
2023-11-14	[diagnostechs]	cuba	<a href="#">Link</a>
2023-11-14	[Execuzen]	alphv	<a href="#">Link</a>
2023-11-05	[Lander County Convention & Tourism Authority]	noescape	<a href="#">Link</a>
2023-11-10	[Carespring]	noescape	<a href="#">Link</a>
2023-11-13	[shopbentley.com]	blackbasta	<a href="#">Link</a>
2023-11-13	[tarltonandson.com]	lockbit3	<a href="#">Link</a>
2023-11-13	[ASM GLOBAL]	alphv	<a href="#">Link</a>
2023-11-13	[portadelaidefc]	cuba	<a href="#">Link</a>
2023-11-13	[St. Lucie County Tax Collector's]	alphv	<a href="#">Link</a>
2023-11-10	[Bartec Top Holding GmbH]	hunters	<a href="#">Link</a>
2023-11-09	[Garr Silpe, P.C.]	hunters	<a href="#">Link</a>
2023-11-06	[United Africa Group Ltd.]	hunters	<a href="#">Link</a>
2023-11-12	[IDESSA group, S.A. De C.V.]	hunters	<a href="#">Link</a>
2023-11-12	[DrilMaco]	hunters	<a href="#">Link</a>
2023-11-03	[Builders Hardware and Hollow Metal, Inc.]	hunters	<a href="#">Link</a>
2023-11-13	[Homeland Inc.]	hunters	<a href="#">Link</a>
2023-11-03	[Deegenbergklinik]	hunters	<a href="#">Link</a>
2023-11-12	[Owens Group]	hunters	<a href="#">Link</a>
2023-11-13	[TCI Co., Ltd.]	hunters	<a href="#">Link</a>
2023-11-03	[Medjet]	hunters	<a href="#">Link</a>
2023-11-13	[United Site Services]	bianlian	<a href="#">Link</a>
2023-11-13	[NSEIT LIMITED]	bianlian	<a href="#">Link</a>
2023-11-13	[Moneris Solutions]	medusa	<a href="#">Link</a>
2023-11-12	[muellersystems.com]	lockbit3	<a href="#">Link</a>
2023-11-13	[msim.de]	lockbit3	<a href="#">Link</a>
2023-11-02	[Putzel Electrical Contractors Inc]	noescape	<a href="#">Link</a>
2023-11-12	[aegean.gr]	lockbit3	<a href="#">Link</a>
2023-11-12	[thewalkerschool.org]	lockbit3	<a href="#">Link</a>
2023-11-12	[modafabrics.com]	lockbit3	<a href="#">Link</a>
2023-11-12	[wombleco.com]	lockbit3	<a href="#">Link</a>
2023-11-12	[cityofclarksville.com]	lockbit3	<a href="#">Link</a>
2023-11-12	[digitaldruck-esser.de]	lockbit3	<a href="#">Link</a>
2023-11-12	[hotelemc2.com]	lockbit3	<a href="#">Link</a>
2023-11-12	[carsonteam.com]	lockbit3	<a href="#">Link</a>
2023-11-12	[plati.it]	lockbit3	<a href="#">Link</a>
2023-11-12	[hotel-ampere-paris.com]	lockbit3	<a href="#">Link</a>
2023-11-12	[Pricesmart]	alphv	<a href="#">Link</a>
2023-11-11	[roth-werkzeugbau.de]	lockbit3	<a href="#">Link</a>
2023-11-11	[heinrichseegers.de]	lockbit3	<a href="#">Link</a>
2023-11-11	[aten.com]	lockbit3	<a href="#">Link</a>
2023-11-11	[quifatex.com]	lockbit3	<a href="#">Link</a>
2023-11-11	[vital.co.za]	lockbit3	<a href="#">Link</a>
2023-11-11	[creatz3d.sg]	lockbit3	<a href="#">Link</a>
2023-11-11	[loiret.fr]	lockbit3	<a href="#">Link</a>
2023-11-05	[PAR Group Co]	noescape	<a href="#">Link</a>
2023-11-11	[MHM Health]	rhysida	<a href="#">Link</a>
2023-11-11	[estes-express.com]	lockbit3	<a href="#">Link</a>
2023-11-11	[shawneemilling.com]	abyss	<a href="#">Link</a>
2023-11-11	[motordepot.co.uk]	abyss	<a href="#">Link</a>
2023-11-11	[Dragos Inc]	alphv	<a href="#">Link</a>
2023-11-10	[floortex.com]	lockbit3	<a href="#">Link</a>
2023-11-10	[planning.org]	lockbit3	<a href="#">Link</a>
2023-11-10	[ayakitchens.com]	blackbasta	<a href="#">Link</a>
2023-11-10	[browardfactory.com]	blackbasta	<a href="#">Link</a>
2023-11-10	[boslogistics.eu]	blackbasta	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-10	[morningstarco.com]	lockbit3	Link
2023-11-10	[Mariposa Landscapes, Inc]	alphv	Link
2023-11-10	[Azienda Ospedaliera Universitaria Integrata di Verona]	rhysida	Link
2023-11-10	[aei.cc]	lockbit3	Link
2023-11-09	[Sinotech Group Taiwan]	alphv	Link
2023-11-09	[Rudolf Venture Chemical Inc - Press Release]	monti	Link
2023-11-09	[Magsaysay Maritime - Press Release]	monti	Link
2023-11-09	[SALUS Controls]	akira	Link
2023-11-09	[Battle Motors (CraneCarrier, CCC)]	akira	Link
2023-11-09	[gotocfr.com]	lockbit3	Link
2023-11-09	[City Furniture Hire]	akira	Link
2023-11-09	[Autocommerce]	akira	Link
2023-11-02	[Koh Brothers]	lorenz	Link
2023-11-09	[Cogdell Memorial Hospital]	lorenz	Link
2023-11-09	[Simons Petroleum/Maxum Petroleum/Pilot Thomas Logistics]	akira	Link
2023-11-09	[ggarabia.com]	lockbit3	Link
2023-11-08	[JS Hovnanian & Sons]	play	Link
2023-11-08	[Identification Products]	play	Link
2023-11-08	[M.R. Williams]	play	Link
2023-11-08	[DESIGNA Verkehrsleittechnik]	play	Link
2023-11-08	[The Supply Room Companies & Citron WorkSpaces]	play	Link
2023-11-08	[Ackerman-Estvold]	play	Link
2023-11-08	[Meindl]	play	Link
2023-11-08	[Conditioned Air]	play	Link
2023-11-08	[Inclinator]	play	Link
2023-11-08	[Crown Supply Co]	play	Link
2023-11-08	[fawry.com]	lockbit3	Link
2023-11-08	[amberhillgroup.com]	lockbit3	Link
2023-11-08	[califanocarrelli.it]	blackbasta	Link
2023-11-08	[sheehyware.com]	alphv	Link
2023-11-08	[Michael Garron Hospital]	akira	Link
2023-11-08	[foley.k12.mn.us]	lockbit3	Link
2023-11-08	[gitiusa.com]	lockbit3	Link
2023-11-08	[allenoverly.com]	lockbit3	Link
2023-11-08	[NeoDomos]	ciphbit	Link
2023-11-07	[Bakrie Group & Bakrie Sumatera Plantations]	alphv	Link
2023-11-07	[Indah Water Konsortium]	rhysida	Link
2023-11-07	[Access to the large database of a US Medical organization]	everest	Link
2023-11-07	[h-tube.com]	blackbasta	Link
2023-11-07	[torrescpa.com]	blackbasta	Link
2023-11-07	[tt-engineering.nl]	blackbasta	Link
2023-11-07	[nicecloud.nl]	blackbasta	Link
2023-11-07	[triflex.nl]	blackbasta	Link
2023-11-07	[cozwolle.nl]	blackbasta	Link
2023-11-07	[Certified Mortgage Planners]	alphv	Link
2023-11-07	[BioPower SustainableEnergy Corporation]	akira	Link
2023-11-07	[BITZER]	akira	Link
2023-11-07	[acawtrustfunds.ca]	blackbasta	Link
2023-11-07	[secci.ca]	blackbasta	Link
2023-11-07	[Hopewell Area School District]	medusa	Link
2023-11-07	[panaya]	cuba	Link
2023-11-07	[prime-art]	cuba	Link
2023-11-07	[ccdrc.pt]	lockbit3	Link
2023-11-07	[Yuxin Automobile Co.Ltd ]	ragroup	Link
2023-11-07	[Aceromex (Unpay-Start Leaking)]	ragroup	Link
2023-11-07	[Japan Aviation Electronics Industry, Ltd]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-06	[sacksteinlaw.com]	blackbasta	Link
2023-11-06	[good-lawyer.com]	lockbit3	Link
2023-11-06	[EFU Life Assurance]	incransom	Link
2023-11-06	[kbrlaw.com]	lockbit3	Link
2023-11-06	[eyephy.com]	lockbit3	Link
2023-11-06	[Mount St. Mary's Seminary]	rhysida	Link
2023-11-06	[concretevalue.com]	lockbit3	Link
2023-11-06	[howlandlaw.net]	lockbit3	Link
2023-11-06	[GEOCOM]	cactus	Link
2023-11-06	[MultiMasters]	cactus	Link
2023-11-06	[UTI Group]	cactus	Link
2023-11-06	[Comfloresta]	alphv	Link
2023-11-05	[Currax Pharmaceuticals]	alphv	Link
2023-11-05	[Advarra leak]	alphv	Link
2023-11-05	[Weidmann & Associates]	medusa	Link
2023-11-05	[Unimed Blumenau]	medusa	Link
2023-11-05	[Leaguers]	medusa	Link
2023-11-05	[Zon Beachside]	medusa	Link
2023-11-05	[Canadian Psychological Association]	medusa	Link
2023-11-05	[Corsica-Ferries]	alphv	Link
2023-11-05	[penanshin]	alphv	Link
2023-11-05	[lathamcenters.org]	abyss	Link
2023-11-05	[Assurius.be]	qilin	Link
2023-11-05	[unique-relations.at]	qilin	Link
2023-11-05	[SMH Group]	rhysida	Link
2023-11-05	[nckb.com]	lockbit3	Link
2023-11-05	[egco.com]	lockbit3	Link
2023-11-05	[benya.capital]	lockbit3	Link
2023-11-05	[global-value-web.com]	lockbit3	Link
2023-11-05	[aseankorea.org]	lockbit3	Link
2023-11-05	[brlogistics.net]	lockbit3	Link
2023-11-05	[bresselouhannaiseintercom.fr]	lockbit3	Link
2023-11-05	[nfcc.gov.my]	lockbit3	Link
2023-11-05	[sansasecurity.com]	lockbit3	Link
2023-11-05	[emiliacentrale.it]	lockbit3	Link
2023-11-05	[letillet.btprms.com]	lockbit3	Link
2023-11-05	[ospedalecoq.it]	lockbit3	Link
2023-11-05	[springeroil.com]	lockbit3	Link
2023-11-05	[szutest.cz]	lockbit3	Link
2023-11-05	[mat-antriebstechnik.de]	lockbit3	Link
2023-11-05	[studio483.com]	lockbit3	Link
2023-11-04	[infosysbpm.com]	lockbit3	Link
2023-11-04	[tks.co.th]	lockbit3	Link
2023-11-03	[GeoPoint Surveying]	play	Link
2023-11-03	[APERS]	ciphbit	Link
2023-11-03	[translink.se]	lockbit3	Link
2023-11-03	[tasl.co.th]	lockbit3	Link
2023-11-03	[abhmf.com]	lockbit3	Link
2023-11-03	[Livability]	incransom	Link
2023-11-03	[portlandtractor.com]	lockbit3	Link
2023-11-03	[unimed.coop.br]	lockbit3	Link
2023-11-03	[jewell.edu]	lockbit3	Link
2023-11-03	[microtrain.net]	lockbit3	Link
2023-11-02	[Warning to Advarra & Gadi!]	alphv	Link
2023-11-01	[Bry-Air]	play	Link
2023-11-02	[JDRM Engineering]	play	Link
2023-11-02	[Craft-Maid]	play	Link
2023-11-02	[Hilyard's]	play	Link
2023-11-02	[North Dakota Grain Inspection Services]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-02	[Gsp Components]	play	<a href="#">Link</a>
2023-11-02	[Ricardo]	play	<a href="#">Link</a>
2023-11-02	[bindagroup.com]	lockbit3	<a href="#">Link</a>
2023-11-02	[lafase.cl]	lockbit3	<a href="#">Link</a>
2023-11-02	[shimano.com]	lockbit3	<a href="#">Link</a>
2023-11-02	[Contact Cottrell and McCullough]	alphv	<a href="#">Link</a>
2023-11-02	[psmicorp.com]	lockbit3	<a href="#">Link</a>
2023-11-02	[imancorp.es]	blackbasta	<a href="#">Link</a>
2023-11-02	[AF Supply]	alphv	<a href="#">Link</a>
2023-11-02	[GO! Handelsschool Aalst]	rhysida	<a href="#">Link</a>
2023-11-01	[Groupe Faubourg]	8base	<a href="#">Link</a>
2023-11-02	[HAL Allergy]	alphv	<a href="#">Link</a>
2023-11-01	[Detroit Symphony Orchestra]	snatch	<a href="#">Link</a>
2023-11-02	[degregoris.com]	lockbit3	<a href="#">Link</a>
2023-11-02	[Bluewater Health (CA) and others]	daixin	<a href="#">Link</a>
2023-11-01	[vitaresearch.com]	lockbit3	<a href="#">Link</a>
2023-11-01	[sanmiguel.iph]	lockbit3	<a href="#">Link</a>
2023-11-01	[steelofcarolina.com]	lockbit3	<a href="#">Link</a>
2023-11-01	[raumberg-gumpenstein.at]	lockbit3	<a href="#">Link</a>
2023-11-01	[kitprofs.com]	lockbit3	<a href="#">Link</a>
2023-11-01	[imprex.es]	lockbit3	<a href="#">Link</a>
2023-11-01	[Hawkeye Area Community Action Program, Inc]	blacksuit	<a href="#">Link</a>
2023-11-01	[Advarra Inc]	alphv	<a href="#">Link</a>
2023-11-01	[summithealth.com]	lockbit3	<a href="#">Link</a>
2023-11-01	[US Claims Solutions]	knight	<a href="#">Link</a>
2023-11-01	[strongtie.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[ampersand.tv]	blackbasta	<a href="#">Link</a>
2023-11-01	[baccarat.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[piemmeonline.it]	blackbasta	<a href="#">Link</a>
2023-11-01	[fortive.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[gannons.co.uk]	blackbasta	<a href="#">Link</a>
2023-11-01	[gsp.com.br]	blackbasta	<a href="#">Link</a>
2023-11-01	[TANATEX Chemicals]	metaencryptor	<a href="#">Link</a>
2023-11-01	[edwardian.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[bionpharma.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[stantonwilliams.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[hugohaeffner.com]	blackbasta	<a href="#">Link</a>
2023-11-01	[intred.it]	blackbasta	<a href="#">Link</a>
2023-11-01	[Town of Iowa]	alphv	<a href="#">Link</a>
2023-11-01	[Traxall France]	8base	<a href="#">Link</a>
2023-11-01	[Armstrong Consultants]	8base	<a href="#">Link</a>
2023-11-01	[JAI A/S]	8base	<a href="#">Link</a>
2023-11-01	[Schöler Fördertechnik AG]	8base	<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.