



Ausgabe: 20231129

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	Link
CVE-2023-46747	0.965530000	0.995020000	Link
CVE-2023-46604	0.966470000	0.995360000	Link
CVE-2023-42793	0.972640000	0.998130000	Link
CVE-2023-38035	0.970400000	0.996950000	Link
CVE-2023-35078	0.963180000	0.994120000	Link
CVE-2023-34362	0.928450000	0.987830000	Link
CVE-2023-34039	0.925730000	0.987500000	Link
CVE-2023-33246	0.970860000	0.997160000	Link
CVE-2023-32315	0.957520000	0.992650000	Link
CVE-2023-30625	0.936230000	0.988790000	Link
CVE-2023-30013	0.925700000	0.987500000	Link
CVE-2023-28771	0.918550000	0.986590000	Link
CVE-2023-27372	0.971190000	0.997320000	Link
CVE-2023-27350	0.972290000	0.997940000	Link
CVE-2023-26469	0.915280000	0.986200000	Link
CVE-2023-26360	0.913940000	0.986060000	Link
CVE-2023-25717	0.962680000	0.993930000	Link
CVE-2023-25194	0.910980000	0.985730000	Link
CVE-2023-2479	0.958820000	0.992960000	Link
CVE-2023-24489	0.969450000	0.996590000	Link
CVE-2023-22518	0.967630000	0.995850000	Link
CVE-2023-22515	0.955290000	0.992100000	Link
CVE-2023-21839	0.956630000	0.992440000	Link
CVE-2023-21823	0.955130000	0.992050000	Link
CVE-2023-21554	0.961220000	0.993530000	Link
CVE-2023-20887	0.950720000	0.991160000	Link
CVE-2023-1671	0.952600000	0.991540000	Link
CVE-2023-0669	0.966380000	0.995330000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 28 Nov 2023

[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um einen Cross-Site

Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- [Link](#)

Tue, 28 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](#)

Tue, 28 Nov 2023

[UPDATE] [kritisch] Perl: Schwachstelle ermöglicht Privilegieneskalation

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

- [Link](#)

Tue, 28 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](#)

Tue, 28 Nov 2023

[UPDATE] [hoch] Kubernetes: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Kubernetes ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Tue, 28 Nov 2023

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

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

- [Link](#)

Tue, 28 Nov 2023

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Tue, 28 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](#)

Tue, 28 Nov 2023

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

Tue, 28 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](#)

Tue, 28 Nov 2023

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

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

- [Link](#)

Tue, 28 Nov 2023

[NEU] [hoch] SolarWinds Platform: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in SolarWinds Platform ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 28 Nov 2023

[NEU] [hoch] IBM Security Guardium: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM Security Guardium ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 27 Nov 2023

[NEU] [hoch] OTRS: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonym Angreifer kann eine Schwachstelle in OTRS ausnutzen, um Informationen offenzulegen.

- [Link](#)

Mon, 27 Nov 2023

[UPDATE] [hoch] poppler: Mehrere Schwachstellen ermöglichen Denial of Service

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

- [Link](#)

Mon, 27 Nov 2023

[UPDATE] [hoch] poppler: Schwachstelle ermöglicht Code Ausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in poppler ausnutzen, um einen Denial of Service Angriff durchzuführen und möglicherweise Code mit den Privilegien des angegriffenen Benutzers auszuführen.

- [Link](#)

Mon, 27 Nov 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 27 Nov 2023

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

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

- [Link](#)

Mon, 27 Nov 2023

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

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

- [Link](#)

Mon, 27 Nov 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge

ausnutzen, um beliebigen Code auszuführen.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/28/2023	[Tenda AC Router Stack Buffer Overflow (CVE-2021-31755)]	critical
11/28/2023	[Tenda AC Router RCE (CVE-2020-10987)]	critical
11/28/2023	[Google Chrome < 119.0.6045.199 Multiple Vulnerabilities]	critical
11/28/2023	[Google Chrome < 119.0.6045.199 Multiple Vulnerabilities]	critical
11/28/2023	[Apache Tomcat 8.5.0 < 8.5.96]	critical
11/28/2023	[Apache Tomcat 9.0.0.M1 < 9.0.83]	critical
11/28/2023	[Apache Tomcat 10.1.0.M1 < 10.1.16]	critical
11/28/2023	[RHEL 8 : fence-agents (RHSA-2023:7523)]	critical
11/28/2023	[Ubuntu 22.04 LTS : Linux kernel (StarFive) vulnerabilities (USN-6520-1)]	critical
11/28/2023	[Ubuntu 22.04 LTS : Linux kernel (NVIDIA) vulnerabilities (USN-6502-3)]	critical
11/28/2023	[Fedora 37 : python-geopandas (2023-8857bdcd95)]	critical
11/28/2023	[Fedora 39 : python-geopandas (2023-1c5e667fd0)]	critical
11/28/2023	[Fedora 38 : python-geopandas (2023-c907492c3e)]	critical
11/28/2023	[Fedora 38 : openvpn (2023-e4df33666c)]	critical
11/28/2023	[Oracle Linux 9 : dotnet8.0 (ELSA-2023-7253)]	critical
11/28/2023	[Rocky Linux 8 : dotnet6.0 (RLSA-2023:7258)]	critical
11/28/2023	[Rocky Linux 8 : nodejs:20 (RLSA-2023:7205)]	critical
11/28/2023	[Rocky Linux 8 : dotnet7.0 (RLSA-2023:7256)]	critical
11/28/2023	[RHEL 8 : kernel (RHSA-2023:7549)]	high
11/28/2023	[RHEL 8 : kernel-rt (RHSA-2023:7551)]	high
11/28/2023	[RHEL 9 : postgresql (RHSA-2023:7545)]	high
11/28/2023	[RHEL 8 : kernel-rt (RHSA-2023:7548)]	high
11/28/2023	[RHEL 8 : firefox (RHSA-2023:7547)]	high
11/28/2023	[RHEL 8 : tigervnc (RHSA-2023:7526)]	high
11/28/2023	[Oracle Linux 9 : firefox (ELSA-2023-7507)]	high
11/28/2023	[Oracle Linux 9 : thunderbird (ELSA-2023-7501)]	high
11/28/2023	[Oracle Linux 7 : thunderbird (ELSA-2023-7505)]	high
11/28/2023	[Debian DLA-3672-1 : postgresql-multicorn - LTS update]	high
11/28/2023	[Debian DLA-3671-1 : mediawiki - LTS security update]	high
11/28/2023	[RHEL 8 : kpatch-patch (RHSA-2023:7559)]	high
11/28/2023	[Fedora 39 : libcap (2023-ad944c2d34)]	high
11/28/2023	[Fedora 38 : golang-github-nats-io / golang-github-nats-io-jwt-2 / etc (2023-66966ae3d0)]	high
11/28/2023	[Fedora 39 : golang-github-nats-io / golang-github-nats-io-jwt-2 / etc (2023-3a895ff65c)]	high
11/28/2023	[RHEL 8 : kpatch-patch (RHSA-2023:7554)]	high
11/28/2023	[RHEL 8 : kernel (RHSA-2023:7557)]	high
11/28/2023	[Rocky Linux 8 : thunderbird (RLSA-2023:7500)]	high
11/28/2023	[Rocky Linux 8 : open-vm-tools (RLSA-2023:7265)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Tue, 28 Nov 2023

Fortra Digital Guardian Agent Uninstaller Cross Site Scripting / UninstallKey Cached

The uninstaller in Fortra Digital Guardian Agent versions prior to 7.9.4 suffers from a cross site scripting vulnerability. Additionally, the Agent Uninstaller handles sensitive data insecurely and caches the Uninstall key in memory. This key can be used to stop or uninstall the application. This allows a locally authenticated attacker with administrative privileges to disable the application temporarily or even remove the application from the system completely.

- [Link](#)

” “Tue, 28 Nov 2023

etcd-browser 87ae63d75260 Directory Traversal

etcd-browser version 87ae63d75260 suffers from a directory traversal vulnerability.

- [Link](#)

” “Tue, 28 Nov 2023

Loytec L-INX Automation Servers Information Disclosure / Cleartext Secrets

Loytec LINX-151 with firmware version 7.2.4 and LINX-212 with firmware version 6.2.4 suffer from file disclosure vulnerabilities that leak secrets as well as issues with storing secrets in the clear.

- [Link](#)

” “Tue, 28 Nov 2023

Loytec LINX Configurator 7.4.10 Insecure Transit / Cleartext Secrets

Loytec LINX Configurator version 7.4.10 suffers from insecure transit and cleartext hardcoded secret vulnerabilities.

- [Link](#)

” “Tue, 28 Nov 2023

WebRTC PacketRouter Dangling Entry

A dangling pointer vulnerability is present in WebRTC’s PacketRouter due to an SDP SIM group SSRC from one track (e.g., video) colliding with an existing SSRC from a different track (e.g., audio). This inconsistency between the `send_modules_map` and the `send_modules_list` can lead to a use after free.

- [Link](#)

” “Tue, 28 Nov 2023

m-privacy TightGate-Pro Code Execution / Insecure Permissions

m-privacy TightGate-Pro suffers from code execution, insecure permissions, deletion mitigation, and outdated server vulnerabilities.

- [Link](#)

” “Tue, 28 Nov 2023

SmartNode SN200 3.21.2-23021 OS Command Injection

SmartNode SN200 versions 3.21.2-23021 and below suffer from a remote command execution vulnerability.

- [Link](#)

” “Mon, 27 Nov 2023

TitanNit Web Control 2.01 / Atemio 7600 Root Remote Command Execution

The Atemio AM 520 HD Full HD satellite receiver has a vulnerability that enables an unauthorized attacker to execute system commands with elevated privileges. This exploit is facilitated through the use of the `getcommand` query within the application, allowing the attacker to gain root access. Firmware versions 2.01 and below are affected.

- [Link](#)

” “Mon, 27 Nov 2023

osCommerce 4 Cross Site Scripting

osCommerce version 4 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 27 Nov 2023

PopojiCMS 2.0.1 Remote Command Execution

PopojiCMS version 2.0.1 suffers from a remote command execution vulnerability.

- [Link](#)

” “Mon, 27 Nov 2023

CSZ CMS 1.3.0 Remote Command Execution

CSZ CMS version 1.3.0 suffers from a remote command execution vulnerability. Exploit written in Python.

- [Link](#)

” “Mon, 27 Nov 2023

CE Phoenix 1.0.8.20 Remote Command Execution

CE Phoenix version 1.0.8.20 suffers from an authenticated remote command execution vulnerability.

- [Link](#)

” “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](#)

”

0-Days der letzten 5 Tage

“Mon, 27 Nov 2023

ZDI-23-1751: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1750: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1749: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1748: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1747: Adobe Acrobat Reader DC Font Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1746: Adobe Acrobat Reader DC Font Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1745: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1744: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1743: Adobe Acrobat Reader DC Font Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1742: Adobe Acrobat Reader DC Font Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1741: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1740: Adobe Acrobat Reader DC Font Parsing Memory Corruption Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1739: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1738: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1737: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1736: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1735: Fuji Electric Tellus Lite V-Simulator V9 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1734: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1733: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1732: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1731: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1730: Fuji Electric Tellus Lite Incorrect Default Permissions Local Privilege Escalation Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1729: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1728: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1727: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1726: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1725: Fuji Electric Tellus Lite V-Simulator V9 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1724: Fuji Electric Tellus Lite V-Simulator V9 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1723: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1722: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1721: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Mon, 27 Nov 2023

ZDI-23-1720: Fuji Electric Tellus Lite V-Simulator 6 V9 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

”

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
2023-11-28	Grimme	[DEU]	Link
2023-11-27	Prefeitura de Taboão da Serra	[BRA]	Link
2023-11-27	Ministerio de Finanzas Públicas (Minfin)	[GTM]	Link
2023-11-27	North Texas Municipal Water District	[USA]	Link
2023-11-25	HSE (Holding Slovenske Elektrarne)	[SVN]	Link
2023-11-25	AVU (Energieversorger)	[DEU]	Link
2023-11-24	Ardent Health Services	[USA]	Link
2023-11-23	Zweckverband gemeindliche Datenverarbeitung im Kreis Neu-Ulm	[DEU]	Link
2023-11-22	Véligo Location	[FRA]	Link
2023-11-22	Gemeinde Zollikofen	[CHE]	Link
2023-11-22	Svenska kyrkan (l'Église suédoise)	[SWE]	Link
2023-11-22	New Relic	[USA]	Link
2023-11-19	Rostocker Straßenbahn AG (RSAG)	[DEU]	Link
2023-11-18	Fidelity National Financial (FNF)	[USA]	Link
2023-11-17	SIAAP (Syndicat Interdépartemental pour l'Assainissement de l'Agglomération Parisienne)	[FRA]	Link
2023-11-17	Mössinger Stadtverwaltung	[DEU]	Link
2023-11-17	Gellyberry Studios	[SWE]	Link
2023-11-16	Etelä-Savon ammattiopisto Esedu	[FIN]	Link
2023-11-16	Sabre Insurance Group	[GBR]	Link
2023-11-15	Meredosia-Chambersburg school district	[USA]	Link
2023-11-14	Bladen County Government	[USA]	Link
2023-11-14	North Muskegon Public Schools	[USA]	Link
2023-11-14	Beaverton School District	[USA]	Link
2023-11-14	City of Long Beach	[USA]	Link
2023-11-14	King Edward VII's Hospital	[GBR]	Link
2023-11-13	Yanfeng	[CHN]	Link
2023-11-13	North Carolina Central University (NCCU)	[USA]	Link
2023-11-12	Huber Heights	[USA]	Link
2023-11-12	Tunstall	[NLD]	Link
2023-11-12	Deutsche Energie-Agentur (Dena)	[DEU]	Link
2023-11-11	Okada Manila	[PHL]	Link
2023-11-10	DP World Australia	[AUS]	Link
2023-11-10	Derichebourg Multiservices	[FRA]	Link
2023-11-10	Glendale Community College (GCC)	[USA]	Link
2023-11-09	Industrial and Commercial Bank of China (ICBC)	[CHN]	Link
2023-11-09	Tri-City Medical Center	[USA]	Link
2023-11-09	Henry County Schools	[USA]	Link
2023-11-08	York Region District School Board	[CAN]	Link
2023-11-08	Hellenic Public Properties Company (ETAD)	[GRC]	Link
2023-11-07	Comhairle nan Eilean Siar	[GBR]	Link
2023-11-07	Harris Center for Mental Health and IDD	[USA]	Link
2023-11-07	Washington State Department of Transportation (WSDOT)	[USA]	Link
2023-11-06	KaDeWe	[DEU]	Link
2023-11-05	Le conseil départemental du Loiret	[FRA]	Link
2023-11-05	Madison Memorial Hospital	[USA]	Link
2023-11-05	Pulaski County Public Schools (PCPS)	[USA]	Link
2023-11-05	Concevis AG	[CHE]	Link
2023-11-04	Butte School District	[USA]	Link
2023-11-02	Infosys McCamish Systems	[USA]	Link
2023-11-02	Crystal Run Healthcare	[USA]	Link
2023-11-01	Mr. Cooper Group	[USA]	Link
2023-11-01	Rekord Fenster Türen	[DEU]	Link
2023-11-01	EDC	[DNK]	Link

Datum	Opfer	Land	Information
2023-11-01	Cogdell Memorial Hospital	[USA]	Link

Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-28	[Incisive Media]	8base	Link
2023-11-28	[Honey Birdette]	8base	Link
2023-11-28	[GOLDMUND]	8base	Link
2023-11-28	[Wild Republic]	8base	Link
2023-11-28	[Groupe Apex-Isast]	8base	Link
2023-11-28	[Leezer Agency]	8base	Link
2023-11-28	[Cimbali National Accounts]	8base	Link
2023-11-28	[Fortiss LLC]	8base	Link
2023-11-28	[Noble Mountain Tree Farm]	play	Link
2023-11-28	[nal.res.in]	lockbit3	Link
2023-11-28	[dawsongroup.uk]	lockbit3	Link
2023-11-28	[hi-schoolpharmacy.com]	lockbit3	Link
2023-11-28	[EDGE Realty Partners]	play	Link
2023-11-28	[SurvTech Solutions]	play	Link
2023-11-28	[Byfod]	play	Link
2023-11-28	[Retailer Web Services]	play	Link
2023-11-28	[Sparex]	play	Link
2023-11-28	[Continental Shipping Line]	play	Link
2023-11-28	[MooreCo]	play	Link
2023-11-28	[AMERICAN INSULATED GLASS]	play	Link
2023-11-28	[Elston-nationwide]	play	Link
2023-11-28	[Thillens]	play	Link
2023-11-28	[SinglePoint Outsourcing]	play	Link
2023-11-28	[China Petrochemical Development]	alphv	Link
2023-11-28	[First Housing Development]	hunters	Link
2023-11-28	[JD Sprinter Holdings 2010 SL]	metaencrytor	Link
2023-11-28	[FYIdoctors]	cactus	Link
2023-11-28	[Axiom Construction & Consulting]	cactus	Link
2023-11-28	[Medi-Market]	cactus	Link
2023-11-28	[Odalys Vacances]	cactus	Link
2023-11-28	[North Texas Municipal Water District (US)]	daixin	Link
2023-11-27	[Yanfeng]	qilin	Link
2023-11-27	[Bangkok University]	rhysida	Link
2023-11-27	[NC Central University]	rhysida	Link
2023-11-27	[Imt - Press Release]	monti	Link
2023-11-27	[Law Offices of John E Hill - Press Release]	monti	Link
2023-11-27	[stsaviationgroup.com]	lockbit3	Link
2023-11-27	[InstantWhip]	hunters	Link
2023-11-27	[Vertex Resource Group]	alphv	Link
2023-11-27	[Fischione Instruments Inc]	alphv	Link
2023-11-27	[Legacy Mail Management]	akira	Link
2023-11-27	[carrellblanton.com]	threeam	Link
2023-11-27	[Plastic Molding Technology Inc.]	bianlian	Link
2023-11-27	[New River Community & Technical College]	blacksuit	Link
2023-11-27	[Huber Heights]	blacksuit	Link
2023-11-27	[sillslegal]	alphv	Link
2023-11-26	[Katsky Korins]	meow	Link
2023-11-26	[AlJaber Engineering]	ransomexx	Link
2023-11-26	[ALAB laboratoria]	ragroup	Link
2023-11-25	[kenso.com.my]	lockbit3	Link
2023-11-25	[SWISHSMILES.COM]	clop	Link
2023-11-25	[TXWES.EDU]	clop	Link
2023-11-25	[SWEETLAKE.COM]	clop	Link
2023-11-25	[SGMGROUP.COM]	clop	Link
2023-11-25	[MORSKATEMANUFACTURING.COM]	clop	Link
2023-11-24	[Hampton Newport News CSB (Last chance)]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-24	[Energy China]	rhysida	Link
2023-11-18	[TALENTUM Temporal SAS]	noescape	Link
2023-11-24	[carriereindustrial.com]	donutleaks	Link
2023-11-24	[Albert, Righter & Tittmann architechts, inc.]	donutleaks	Link
2023-11-24	[nrtw.org]	lockbit3	Link
2023-11-24	[preidlhof.it]	lockbit3	Link
2023-11-24	[ribolia.com]	lockbit3	Link
2023-11-24	[Lincoln Office]	hunters	Link
2023-11-24	[LCA Consultores]	alphv	Link
2023-11-24	[TJM PRODUCTS PTY. LTD]	alphv	Link
2023-11-24	[Spectrum Solutions LLC]	alphv	Link
2023-11-05	[Es Saadi]	meow	Link
2023-11-05	[Zenithpharma]	meow	Link
2023-11-05	[Back Roads]	meow	Link
2023-11-09	[Equaldex]	meow	Link
2023-11-18	[Vanderbilt University Medical Center]	meow	Link
2023-11-22	[Standard Filter]	meow	Link
2023-11-23	[des-ae.com]	lockbit3	Link
2023-11-23	[unidesign-jewel.com]	lockbit3	Link
2023-11-23	[Eckell Sparks Law Firm]	alphv	Link
2023-11-23	[officinaverdedesign.it]	lockbit3	Link
2023-11-23	[B+P Gerüstbau GmbH]	incransom	Link
2023-11-23	[DM Civil Co.]	incransom	Link
2023-11-23	[Ingo Money Inc]	incransom	Link
2023-11-23	[Nicole Miller]	incransom	Link
2023-11-23	[Pro Metals LLC]	incransom	Link
2023-11-23	[Springfield Area Chamber of Commerce]	incransom	Link
2023-11-23	[Trylon TSF Inc.]	incransom	Link
2023-11-22	[McHale Landscape Design]	play	Link
2023-11-22	[Fidelity National Financial]	alphv	Link
2023-11-22	[Alspec]	akira	Link
2023-11-22	[Custom Engineering & Fabrication, Inc.]	akira	Link
2023-11-22	[IQ Supply Solutions]	akira	Link
2023-11-22	[NESPOLI GROUP]	alphv	Link
2023-11-22	[Community Hospital]	medusa	Link
2023-11-22	[merz-elektro.de]	lockbit3	Link
2023-11-22	[art-eco.it]	lockbit3	Link
2023-11-22	[therobisongroup.com]	lockbit3	Link
2023-11-22	[ds-granit.fr]	threeam	Link
2023-11-21	[APVL ingénierie]	8base	Link
2023-11-21	[Cold Car Spa]	8base	Link
2023-11-21	[La Contabile Spa]	8base	Link
2023-11-21	[DMC Luxembourg]	8base	Link
2023-11-22	[Hills Legal Group Ltd]	8base	Link
2023-11-22	[Brown's Bay Packing Company]	8base	Link
2023-11-22	[Hahn and Clay, Inc.]	8base	Link
2023-11-22	[Imperiali AG]	8base	Link
2023-11-21	[[DATA] Bakrie Group & Bakrie Sumatera Plantations]	alphv	Link
2023-11-21	[floydskerenlaw.com]	lockbit3	Link
2023-11-21	[bnpmmedia.com]	lockbit3	Link
2023-11-21	[Verhelst]	cactus	Link
2023-11-21	[Petersen Health Care]	cactus	Link
2023-11-21	[Paul Stuart]	cactus	Link
2023-11-21	[Crystal Lake Health Center]	hunters	Link
2023-11-21	[qautomotive.com.au]	lockbit3	Link
2023-11-21	[martinique.no]	lockbit3	Link
2023-11-21	[phihydraulics.com]	lockbit3	Link
2023-11-21	[St Edmund's College & Prep School]	rhysida	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-21	[helifrusa.com]	lockbit3	Link
2023-11-21	[Bolidt]	bianlian	Link
2023-11-21	[Growers Express]	bianlian	Link
2023-11-21	[NSEIT Limited (a subsidiary of the National Stock Exchange of India)]	bianlian	Link
2023-11-11	[Rc Moore Inc]	noescape	Link
2023-11-10	[Enware Australia Pty Ltd]	noescape	Link
2023-11-20	[sabre.co.uk]	lockbit3	Link
2023-11-20	[nybravestfcu.org]	lockbit3	Link
2023-11-20	[Hampton Newport News CSB]	alphv	Link
2023-11-20	[jlgmarine.com]	blackbasta	Link
2023-11-12	[Studio D.EL.LA. SRL]	knight	Link
2023-11-14	[Barnett Millworks]	knight	Link
2023-11-20	[Dreyfuss Williams & Associates Co., LPA]	knight	Link
2023-11-20	[onyourmark.org]	lockbit3	Link
2023-11-20	[agrovi.dk]	blackbasta	Link
2023-11-20	[arenaproducts.com]	blackbasta	Link
2023-11-20	[etude-villa.fr]	blackbasta	Link
2023-11-16	[UPDATE! FEAM Maintenance]	alphv	Link
2023-11-20	[brownintegratedlogistics.com]	lockbit3	Link
2023-11-20	[British Library]	rhysida	Link
2023-11-22	[Hahn & Clay, Inc.]	8base	Link
2023-11-19	[Tackle West]	alphv	Link
2023-11-19	[U.L. COLEMAN COMPANIES]	alphv	Link
2023-11-19	[Autonomous Flight - @autonomousfly]	alphv	Link
2023-11-18	[The DMC]	play	Link
2023-11-18	[nealbrothers.co.uk]	threeam	Link
2023-11-18	[generalrefrig.com]	lockbit3	Link
2023-11-17	[PruittHealth]	noescape	Link
2023-11-17	[ajcfood.com]	lockbit3	Link
2023-11-17	[CENTRE D'AUTO P.R.N. SALABERRY IN]	medusa	Link
2023-11-17	[McCray & Withrow]	medusa	Link
2023-11-17	[Metro MPLS]	akira	Link
2023-11-17	[HAESUNG DS CO Ltd]	qilin	Link
2023-11-05	[Kwik Industries, Inc.]	noescape	Link
2023-11-17	[WellLife Network Inc.]	incransom	Link
2023-11-17	[ATC SA]	akira	Link
2023-11-17	[Select Education Group]	blacksuit	Link
2023-11-17	[edc.dk]	blackbasta	Link
2023-11-17	[villanuevadelaserena.es]	lockbit3	Link
2023-11-17	[Admilla ELAP]	ransomexx	Link
2023-11-17	[Aceromex]	ragroup	Link
2023-11-17	[Chung Hwa Chemical Industrial Works]	ragroup	Link
2023-11-17	[SUMMIT VETERINARY PHARMACEUTICALS LIMITED]	ragroup	Link
2023-11-17	[Informist Media]	ragroup	Link
2023-11-17	[Epstein Law]	qilin	Link
2023-11-16	[Toyota Financial]	medusa	Link
2023-11-17	[owensgroup.uk]	lockbit3	Link
2023-11-17	[hsksgreenhalgh.co.uk]	lockbit3	Link
2023-11-17	[krblaw.com]	lockbit3	Link
2023-11-17	[communitydentalme.org]	lockbit3	Link
2023-11-17	[chicagotrading.com]	lockbit3	Link
2023-11-17	[adyne.com]	lockbit3	Link
2023-11-17	[goodhopeholdings.com]	lockbit3	Link
2023-11-17	[planethomelending.com]	lockbit3	Link
2023-11-15	[Decatur Independent School District]	incransom	Link
2023-11-16	[Consilium staffing llc]	incransom	Link
2023-11-15	[Yamaha Motor Philippines,Inc.]	incransom	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-15	[Guardian Alarm]	incransom	Link
2023-11-15	[SCOLARI Srl]	incransom	Link
2023-11-16	[uchlogistics.co.uk]	blackbasta	Link
2023-11-16	[citycontainer.dk]	blackbasta	Link
2023-11-16	[FEAM Maintenance]	alphv	Link
2023-11-16	[thewalkerschool]	alphv	Link
2023-11-15	[MeridianLink fails to file with the SEC..so we do it for them + 24 hours to pay]	alphv	Link
2023-11-15	[EOS]	lorenz	Link
2023-11-15	[THK Co., Ltd.]	hunters	Link
2023-11-15	[Cardinal MetalWorks]	alphv	Link
2023-11-15	[ADH Health Products Inc]	alphv	Link
2023-11-08	[Ingeniería FULCRUM]	8base	Link
2023-11-09	[Scheidt GmbH]	8base	Link
2023-11-15	[Gallagher Tire, Inc.]	8base	Link
2023-11-15	[MODERNGRAB, S.A.]	8base	Link
2023-11-15	[Storey Trucking Company, Inc.]	8base	Link
2023-11-15	[APREVYA]	8base	Link
2023-11-15	[Lanificio Luigi Colombo S.p.A.]	8base	Link
2023-11-15	[MERRILL Technologies Group]	8base	Link
2023-11-15	[Ontario Pork]	8base	Link
2023-11-15	[Parsons Investments]	8base	Link
2023-11-15	[kwhfreeze.fi]	lockbit3	Link
2023-11-14	[PIKE Technologies]	play	Link
2023-11-14	[Proforma Albrecht]	play	Link
2023-11-14	[Fgs]	play	Link
2023-11-14	[Trademark Property]	play	Link
2023-11-14	[Nomot]	play	Link
2023-11-14	[Global Technologies Racing Ltd]	play	Link
2023-11-14	[Thompson Candy]	play	Link
2023-11-14	[Road Scholar Transport]	play	Link
2023-11-14	[KaDeWe]	play	Link
2023-11-14	[Wyatt Detention Center]	play	Link
2023-11-14	[Guntert & Zimmerman]	play	Link
2023-11-14	[ConSpare]	play	Link
2023-11-14	[Premise Health]	alphv	Link
2023-11-15	[MeridianLink]	alphv	Link
2023-11-14	[Gnome Landscapes]	alphv	Link
2023-11-14	[agromatic.de]	blackbasta	Link
2023-11-14	[cmcsheetmetal.com]	blackbasta	Link
2023-11-14	[rekord.de]	blackbasta	Link
2023-11-14	[boulangerieauger.com]	blackbasta	Link
2023-11-14	[maytec.de]	blackbasta	Link
2023-11-14	[SheelaFoam]	alphv	Link
2023-11-14	[Naftor and Grupa Pern (Naftoport/ SIARKOPOL/ SARMATIA/ NAFTOSERWIS) is the most dangerous]	alphv	Link
2023-11-14	[4set.es]	alphv	Link
2023-11-14	[diagnostechs]	cuba	Link
2023-11-14	[Execuzen]	alphv	Link
2023-11-05	[Lander County Convention & Tourism Authority]	noescape	Link
2023-11-10	[Carespring]	noescape	Link
2023-11-13	[shopbentley.com]	blackbasta	Link
2023-11-13	[tarltonandson.com]	lockbit3	Link
2023-11-13	[ASM GLOBAL]	alphv	Link
2023-11-13	[portadelaidefc]	cuba	Link
2023-11-13	[St. Lucie County Tax Collector's]	alphv	Link
2023-11-10	[Bartec Top Holding GmbH]	hunters	Link
2023-11-09	[Garr Silpe, P.C.]	hunters	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-06	[United Africa Group Ltd.]	hunters	Link
2023-11-12	[IDESSA group, S.A. De C.V.]	hunters	Link
2023-11-12	[DrilMaco]	hunters	Link
2023-11-03	[Builders Hardware and Hollow Metal, Inc.]	hunters	Link
2023-11-13	[Homeland Inc.]	hunters	Link
2023-11-03	[Deegenbergklinik]	hunters	Link
2023-11-12	[Owens Group]	hunters	Link
2023-11-13	[TCI Co., Ltd.]	hunters	Link
2023-11-03	[Medjet]	hunters	Link
2023-11-13	[United Site Services]	bianlian	Link
2023-11-13	[NSEIT LIMITED]	bianlian	Link
2023-11-13	[Moneris Solutions]	medusa	Link
2023-11-12	[muellersystems.com]	lockbit3	Link
2023-11-13	[msim.de]	lockbit3	Link
2023-11-02	[Putzel Electrical Contractors Inc]	noescape	Link
2023-11-12	[aegean.gr]	lockbit3	Link
2023-11-12	[thewalkerschool.org]	lockbit3	Link
2023-11-12	[modafabrics.com]	lockbit3	Link
2023-11-12	[wombleco.com]	lockbit3	Link
2023-11-12	[cityofclarksville.com]	lockbit3	Link
2023-11-12	[digitaldruck-esser.de]	lockbit3	Link
2023-11-12	[hotelemc2.com]	lockbit3	Link
2023-11-12	[carsonteam.com]	lockbit3	Link
2023-11-12	[plati.it]	lockbit3	Link
2023-11-12	[hotel-ampere-paris.com]	lockbit3	Link
2023-11-12	[Pricesmart]	alphv	Link
2023-11-11	[roth-werkzeugbau.de]	lockbit3	Link
2023-11-11	[heinrichseegers.de]	lockbit3	Link
2023-11-11	[aten.com]	lockbit3	Link
2023-11-11	[quifatex.com]	lockbit3	Link
2023-11-11	[vital.co.za]	lockbit3	Link
2023-11-11	[creatz3d.sg]	lockbit3	Link
2023-11-11	[loiret.fr]	lockbit3	Link
2023-11-05	[PAR Group Co]	noescape	Link
2023-11-11	[MHM Health]	rhysida	Link
2023-11-11	[estes-express.com]	lockbit3	Link
2023-11-11	[shawneemilling.com]	abyss	Link
2023-11-11	[motordepot.co.uk]	abyss	Link
2023-11-11	[Dragos Inc]	alphv	Link
2023-11-10	[floortex.com]	lockbit3	Link
2023-11-10	[planning.org]	lockbit3	Link
2023-11-10	[ayakitchens.com]	blackbasta	Link
2023-11-10	[browardfactory.com]	blackbasta	Link
2023-11-10	[boslogistics.eu]	blackbasta	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[Inclinators]	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	[NeoDemos]	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	[ccdrp.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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[abhmfg.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
2023-11-02	[Gsp Components]	play	Link
2023-11-02	[Ricardo]	play	Link
2023-11-02	[bindagroup.com]	lockbit3	Link
2023-11-02	[lafase.cl]	lockbit3	Link
2023-11-02	[shimano.com]	lockbit3	Link
2023-11-02	[Contact Cottrell and McCullough]	alphv	Link
2023-11-02	[psmicorp.com]	lockbit3	Link
2023-11-02	[imancorp.es]	blackbasta	Link
2023-11-02	[AF Supply]	alphv	Link
2023-11-02	[GO! Handelsschool Aalst]	rhysida	Link
2023-11-01	[Groupe Faubourg]	8base	Link
2023-11-02	[HAL Allergy]	alphv	Link
2023-11-01	[Detroit Symphony Orchestra]	snatch	Link
2023-11-02	[degregoris.com]	lockbit3	Link
2023-11-02	[Bluewater Health (CA) and others]	daixin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-11-01	[vitaresearch.com]	lockbit3	Link
2023-11-01	[sanmiguel.iph]	lockbit3	Link
2023-11-01	[steelofcarolina.com]	lockbit3	Link
2023-11-01	[raumberg-gumpenstein.at]	lockbit3	Link
2023-11-01	[kitprofs.com]	lockbit3	Link
2023-11-01	[imprex.es]	lockbit3	Link
2023-11-01	[Hawkeye Area Community Action Program, Inc]	blacksuit	Link
2023-11-01	[Advarra Inc]	alphv	Link
2023-11-01	[summithealth.com]	lockbit3	Link
2023-11-01	[US Claims Solutions]	knight	Link
2023-11-01	[strongtie.com]	blackbasta	Link
2023-11-01	[ampersand.tv]	blackbasta	Link
2023-11-01	[baccarat.com]	blackbasta	Link
2023-11-01	[piemmeonline.it]	blackbasta	Link
2023-11-01	[fortive.com]	blackbasta	Link
2023-11-01	[gannons.co.uk]	blackbasta	Link
2023-11-01	[gsp.com.br]	blackbasta	Link
2023-11-01	[TANATEX Chemicals]	metaencryptor	Link
2023-11-01	[edwardian.com]	blackbasta	Link
2023-11-01	[bionpharma.com]	blackbasta	Link
2023-11-01	[stantonwilliams.com]	blackbasta	Link
2023-11-01	[hugohaeffner.com]	blackbasta	Link
2023-11-01	[intred.it]	blackbasta	Link
2023-11-01	[Town of Iowa]	alphv	Link
2023-11-01	[Traxall France]	8base	Link
2023-11-01	[Armstrong Consultants]	8base	Link
2023-11-01	[JAI A/S]	8base	Link
2023-11-01	[Schöler Fördertechnik AG]	8base	Link

Quellen

Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - packetstormsecurity.com
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

Impressum



Herausgeber:

Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail

info@cyberwald.com

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