Cybersecurity Morgenreport

Ausgabe: 20231201

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

Apache ActiveMQ: Mehrere Codeschmuggel-Lücken von Botnetbetreibern ausgenutzt
Die im Oktober veröffentlichten kritischen Sicherheitsprobleme in ActiveMQ nützen nun Botnet-Betreibern. Derweil gibt es ein neues Sicherheitsproblem.
- Link

—

Sicherheitslücke in Hikvision-Kameras und NVR ermöglicht unbefugten Zugriff
Verschiedene Modelle des chinesischen Herstellers gestatteten Angreifern den unbefugten Zugriff. Auch andere Marken sind betroffen, Patches stehen bereit.
- Link

—

Sicherheitslücke: Schadcode-Attacken auf Solarwinds Platform möglich
Die Solarwinds-Entwickler haben zwei Schwachstellen in ihrer Monitoringsoftware geschlossen.
- Link

—

Scans zu kritischer Sicherheitslücke in ownCloud-Plugin
Die Schwachstelle im GraphAPI-Plugin kann zur unfreiwilligen Preisgabe der Admin-Zugangsdaten führen. ownCloud-Admins sollten schnell reagieren.
- Link

—

Jetzt patchen! Attacken auf Google Chrome
Der Webbrowser Chrome ist verwundbar. Die Entwickler haben mehrere Schwachstellen geschlossen.
- Link

—

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 Webbbrowser kann Schadcode schlüpfen. Außerdem wurde der Datenschutz verbessert.
- Link

—

Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-5360	0.967980000	0.995950000	Link
CVE-2023-4966	0.922670000	0.987100000	Link
CVE-2023-46747	0.965530000	0.995020000	Link
CVE-2023-46604	0.968050000	0.995990000	Link
CVE-2023-42793	0.972640000	0.998130000	Link
CVE-2023-38035	0.970940000	0.997190000	Link
CVE-2023-35078	0.958120000	0.992800000	Link
CVE-2023-34362	0.928450000	0.987850000	Link
CVE-2023-34039	0.925730000	0.987530000	Link
CVE-2023-33246	0.971220000	0.997320000	Link
CVE-2023-32315	0.957520000	0.992660000	Link
CVE-2023-30625	0.936230000	0.988810000	Link
CVE-2023-30013	0.936180000	0.988800000	Link
CVE-2023-28771	0.918550000	0.986610000	Link
CVE-2023-27372	0.971190000	0.997310000	Link
CVE-2023-27350	0.972290000	0.997960000	Link
CVE-2023-26469	0.915280000	0.986230000	Link
CVE-2023-26360	0.913940000	0.986060000	Link
CVE-2023-25717	0.962820000	0.994010000	Link
CVE-2023-25194	0.910980000	0.985740000	Link
CVE-2023-2479	0.958820000	0.992980000	Link
CVE-2023-24489	0.969450000	0.996590000	Link
CVE-2023-22518	0.967630000	0.995850000	Link
CVE-2023-22515	0.955290000	0.992120000	Link
CVE-2023-21839	0.956630000	0.992450000	Link
CVE-2023-21823	0.955130000	0.992060000	Link
CVE-2023-21554	0.961220000	0.993550000	Link
CVE-2023-20887	0.952390000	0.991530000	Link
CVE-2023-1671	0.952600000	0.991570000	Link
CVE-2023-0669	0.966380000	0.995340000	Link

BSI - Warn- und Informationsdienst (WID)

Thu, 30 Nov 2023

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Perl ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 30 Nov 2023
[NEU] [hoch] Tenable Security Nessus Network Monitor: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Tenable Security Nessus Network Monitor ausnutzen, um vertrauliche Informationen offenzulegen, beliebigen Code auszuführen oder Dateien zu manipulieren.
- Link
—
Thu, 30 Nov 2023
[NEU] [hoch] Arcserve Unified Data Protection: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Arcserve Unified Data Protection ausnutzen, um beliebigen Code auszuführen, Dateien zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.
- Link
—
Thu, 30 Nov 2023
[UPDATE] [hoch] PostgreSQL JDBC Treiber: Schwachstelle ermöglicht Codeausführung
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle im PostgreSQL JDBC Treiber ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 30 Nov 2023
[UPDATE] [hoch] GIMP: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GIMP ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Thu, 30 Nov 2023
[UPDATE] [hoch] SHA-3 Implementierungen: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in den SHA-3 Implementierungen mehrerer Produkte ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 30 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
—
Thu, 30 Nov 2023
[UPDATE] [hoch] Apache Struts: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Struts ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Thu, 30 Nov 2023
[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Thu, 30 Nov 2023
[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Thu, 30 Nov 2023

[UPDATE] [hoch] Squid: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link

—

Thu, 30 Nov 2023
[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen
Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Thu, 30 Nov 2023
[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.
- Link

—

Thu, 30 Nov 2023
[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Wed, 29 Nov 2023
[NEU] [hoch] Trellix Enterprise Security Manager: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Trellix Enterprise Security Manager ausnutzen, um Dateien zu manipulieren oder beliebigen Programmcode mit Administratorrechten auszuführen.
- Link

—

Wed, 29 Nov 2023
[NEU] [hoch] IBM InfoSphere Information Server: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in IBM InfoSphere Information Server ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Cross-Site-Scripting-Angriffe durchzuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 29 Nov 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Wed, 29 Nov 2023
[UPDATE] [hoch] VMware Tanzu Spring Security: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Wed, 29 Nov 2023
[UPDATE] [hoch] Mozilla Firefox und Mozilla Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

Wed, 29 Nov 2023
[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird

ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.
- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/30/2023	[Fortinet FortiSIEM Remote Unauthenticated OS Command Injection (FG-IR-23-130)]	critical
11/30/2023	[SUSE SLED12 / SLES12 Security Update : freerdp (SUSE-SU-2023:4611-1)]	critical
11/30/2023	[Nessus Network Monitor < 6.3.1 Multiple Vulnerabilities (TNS-2023-43)]	critical
11/30/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6496-2)]	critical
11/30/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6495-2)]	critical
11/30/2023	[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6494-2)]	critical
11/30/2023	[Ubuntu 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6502-4)]	critical
11/29/2023	[Fedora 38 : qbittorrent (2023-185f3e8ad7)]	critical
11/29/2023	[Fedora 38 : gst-devtools / gstreamer1 / gstreamer1-doc / python-gstreamer1 (2023-7bd66f219f)]	critical
11/29/2023	[Fedora 39 : qbittorrent (2023-1bbfc445a2)]	critical
11/29/2023	[Mitsubishi (CVE-2023-29155)]	critical
11/29/2023	[Mitsubishi (CVE-2023-35762)]	critical
11/30/2023	[Trellix Enterprise Security Manager < 11.6.9 Command Injection]	high
11/30/2023	[SolarWinds Platform 2023.3.0 < 2023.4.2 SQLi]	high
11/30/2023	[Zyxel USG / ATP / VPN < 5.37 Multiple Vulnerabilities]	high
11/30/2023	[Progress MOVEit Transfer < 2022.0.9 / 2022.1 < 2022.1.10 / 2023.0 < 2023.0.7 / 2023.1.1 Multiple Vulnerabilities (November 2023)]	high
11/30/2023	[RHEL 9 : postgresql (RHSA-2023:7616)]	high
11/30/2023	[Debian DLA-3674-1 : thunderbird - LTS security update]	high
11/30/2023	[Debian DLA-3677-1 : gimp-dds - LTS security update]	high
11/30/2023	[Debian DLA-3676-1 : libde265 - LTS security update]	high
11/30/2023	[Fedora 39 : java-17-openjdk (2023-b6612f3819)]	high
11/30/2023	[Fedora 39 : golang-github-google-dap (2023-fa2ec3d3e0)]	high
11/30/2023	[Fedora 38 : golang-github-google-dap (2023-548163deb1)]	high
11/30/2023	[Fedora 37 : golang-github-google-dap (2023-c858d2c53b)]	high
11/29/2023	[Fedora 38 : chromium (2023-4e555aedeb)]	high
11/29/2023	[Fedora 38 : libcap (2023-5911638116)]	high
11/29/2023	[Fedora 39 : webkitgtk (2023-8f84dc8e09)]	high
11/29/2023	[Fedora 39 : chromium (2023-145f259a77)]	high
11/29/2023	[Fedora 39 : gnutls (2023-e075ac32be)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Thu, 30 Nov 2023
CE Phoenix 1.0.8.20 Remote Code Execution
CE Phoenix version 1.0.8.20 remote code execution exploit written in Python.
- Link

—

” “Thu, 30 Nov 2023
Online Student Clearance System 1.0 Shell Upload
Online Student Clearance System versions 1.0 and below suffer from a remote shell upload vulnerability.
- Link

—

” “Wed, 29 Nov 2023
WordPress Royal Elementor Addons And Templates Remote Shell Upload
WordPress Royal Elementor Addons and Templates plugin versions prior to 1.3.79 suffer from a remote shell upload vulnerability.
- Link

—

” “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 stories 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
—
”

0-Days der letzten 5 Tage

“Thu, 30 Nov 2023
ZDI-23-1756: Delta Electronics InfraSuite Device Master PlayWaveFile Directory Traversal Information Disclosure Vulnerability
- Link
—
” “Thu, 30 Nov 2023
ZDI-23-1755: Delta Electronics InfraSuite Device Master RunScript Exposed Dangerous Method Remote Code Execution Vulnerability
- Link
—
” “Thu, 30 Nov 2023
ZDI-23-1754: Delta Electronics InfraSuite Device Master Device-DataCollect Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Thu, 30 Nov 2023
ZDI-23-1753: Delta Electronics InfraSuite Device Master Device-Gateway Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Thu, 30 Nov 2023
ZDI-23-1752: Delta Electronics InfraSuite Device Master UploadMedia Directory Traversal Remote Code Execution Vulnerability
- Link
—
” “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: (Dez)

Datum	Opfer	Land	Information
2023-11-30	Drum/Binghamstown Group Water Scheme	[IRL]	Link
2023-11-29	AUSL Modena	[ITA]	Link
2023-11-29	Groupe Guyamier	[FRA]	Link
2023-11-29	Sprinter Sports	[NLD]	Link
2023-11-28	Grimme	[DEU]	Link
2023-11-28	Landkreis Vorpommern-Rügen	[DEU]	Link
2023-11-28	Inros Lackner	[DEU]	Link
2023-11-28	HTC Global Services	[USA]	Link
2023-11-28	Klinikum Esslingen	[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
2023-11-27	Newfound Area School District	[USA]	Link
2023-11-27	Río Grande	[PRI]	Link
2023-11-27	Staples	[USA]	Link
2023-11-26	Compass Group Italia S.p.A.	[ITA]	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
2023-11-24	Capital Health	[USA]	Link
2023-11-23	Zweckverband gemeindliche Datenverarbeitung im Kreis Neu-Ulm	[DEU]	Link
2023-11-23	City of Hendersonville	[USA]	Link
2023-11-23	Quantum Radiology	[AUS]	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
2023-11-20	Tazewell County	[USA]	Link
2023-11-20	LivaNova	[GBR]	Link
2023-11-20	Pfaff	[DEU]	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

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

Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-30	[HTC Global Services]	alphv	Link
2023-11-30	[Rudolf GmbH & Rudolf Venture Chemicals Inc - Press Release]	monti	Link
2023-11-30	[Bauwerk Boen Group]	akira	Link
2023-11-30	[Covenant Care]	hunters	Link
2023-11-30	[FUTURA Fundamentsysteme was hacked]	knight	Link
2023-11-30	[Contitec Empresarial]	knight	Link
2023-11-30	[Wakefield & Associates]	knight	Link
2023-11-30	[DePauw University]	blacksuit	Link
2023-11-30	[aurobindousa.com]	abyss	Link
2023-11-30	[andersonandjones.com]	blackbasta	Link
2023-11-26	[Science History Institute]	noescape	Link
2023-11-10	[Yale Appliance]	8base	Link
2023-11-18	[Verdecora]	noescape	Link
2023-11-29	[Protected: Name is hidden]	medusalocker	Link
2023-11-29	[Chetu]	medusa	Link
2023-11-29	[New River Community Technical College]	blacksuit	Link
2023-11-29	[jacobsfarmdelcabo.com]	blackbasta	Link
2023-11-29	[AQIPA]	alphv	Link
2023-11-29	[skalar.com]	medusalocker	Link
2023-11-29	[Lydall, Inc.]	akira	Link
2023-11-29	[NCCU.EDU]	clop	Link
2023-11-29	[Alpura]	akira	Link
2023-11-04	[ALPS Ltd]	ransomhouse	Link
2023-11-29	[Great Valley School District]	medusa	Link
2023-11-29	[Servicio Móvil]	akira	Link
2023-11-29	[Teleflora]	akira	Link
2023-11-29	[King Edward VII's Hospital]	rhysida	Link
2023-11-29	[masterk.com]	lockbit3	Link
2023-11-17	[Maldives Ports Limited]	snatch	Link
2023-11-17	[Montachusett Regional Vocational Technical School District]	snatch	Link
2023-11-13	[Museum für Naturkunde]	snatch	Link
2023-11-24	[ALVImedica]	snatch	Link
2023-11-24	[Kologik]	snatch	Link
2023-11-24	[Tyson Foods]	snatch	Link
2023-11-27	[Hunt Guillot & Associates]	snatch	Link
2023-11-27	[Canadian Psychological Association]	snatch	Link
2023-11-29	[tcw.com]	lockbit3	Link
2023-11-28	[Canderel Management]	play	Link
2023-11-28	[OLA Consulting Engineers]	play	Link
2023-11-28	[Labtopia]	play	Link
2023-11-28	[SC Hydraulic Engineering]	play	Link
2023-11-28	[Unitransfer]	play	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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]	metaencryptor	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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[bnpmedia.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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2023-11-06	[United Africa Group Ltd.]	hunters	Link
2023-11-12	[IDESA 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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[allenovery.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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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 Lowa]	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.