Cybersecurity Morgenreport

Ausgabe: 20230831

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

Entwickler von Notepad++ ignoriert offensichtlich Sicherheitslücken
Mehrere Sicherheitslücken gefährden den Texteditor Notepad++. Trotz Informationen zu den Lücken und möglichen Fixes steht ein Sicherheitsupdate noch aus.
- Link

—

Kritische Sicherheitslücke in VMware Aria Operations for Networks
VMware schließt Sicherheitslücken in Aria Operations for Networks. Eine gilt als kritisch und erlaubt den Zugriff ohne Anmeldung.
- Link

—

Webbrowser: Google-Chrome-Update stopft hochriskante Sicherheitslücke
Google bessert im Webbrowser Chrome eine als hochriskant eingestufte Schwachstelle aus.
- Link

—

Webbrowser: Neue Firefox-Releases schließen mehrere Sicherheitslücken
Die Mozilla-Entwickler haben die Firefox-Versionen 117, ESR 115.2 und ESR 102.15 herausgegeben, die mehrere teils hochriskante Sicherheitslücken schließen.
- Link

—

Zoho ManageEngine: Schwachstelle erlaubt Umgehen von Mehrfaktorauthentifizierung
In diversen Zoho ManageEngine-Produkten können Angreifer aufgrund einer Sicherheitslücke die Mehrfaktorauthentifizierung umgehen. Updates stehen bereit.
- Link

—

Jetzt patchen! Attacken auf Juniper-Firewalls beobachtet
Sicherheitsforscher haben Schwachstellen in Juniper Firewalls und Switches dokumentiert. Die Lücken nutzen Angreifer bereits aus.
- Link

—

Jetzt updaten! Hochriskante Sicherheitslücken in 7-Zip ermöglichen Codeschmuggel
Das Archiv-Werkzeug 7-Zip schließt mit neuer Version hochriskante Sicherheitslücken. Einen integrierten Update-Mechanismus gibt es nicht. Handarbeit ist nötig.
- Link

—

Sicherheitsupdates: Drupal-Plug-ins mit Schadcode-Lücken
Wenn bestimmte Plug-ins zum Einsatz kommen, sind mit dem CMS Drupal erstellte Websites attackierbar.
- Link

—

FBI-Warnung: Barracuda ESG-Updates unwirksam, Appliances sofort entfernen
Das FBI warnt vor den Barracuda-ESG-Schwachstellen, die Ende Mai bekannt wurden. Es geht davon aus, dass alle Geräte kompromittiert seien.
- Link

—

Jetzt patchen! Angreifer platzieren Backdoors auf Openfire-Servern
Derzeit gibt es Attacken auf Openfire-Server. Patches sind verfügbar. IT-Sicherheitsforscher warnen vor tausenden angreifbaren Systemen.
- 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-2023-39143	0.921370000	0.985630000	Link
CVE-2023-38035	0.918170000	0.985310000	Link
CVE-2023-3519	0.911990000	0.984750000	Link
CVE-2023-35078	0.965240000	0.994140000	Link
CVE-2023-34362	0.936790000	0.987700000	Link
CVE-2023-33246	0.963860000	0.993610000	Link
CVE-2023-32315	0.963250000	0.993430000	Link
CVE-2023-28771	0.917110000	0.985190000	Link
CVE-2023-28121	0.937820000	0.987810000	Link
CVE-2023-27372	0.970840000	0.996650000	Link
CVE-2023-27350	0.970860000	0.996670000	Link
CVE-2023-26360	0.908440000	0.984420000	Link
CVE-2023-25717	0.965660000	0.994380000	Link
CVE-2023-25194	0.924830000	0.986000000	Link
CVE-2023-24489	0.967300000	0.995060000	Link
CVE-2023-21839	0.961720000	0.992920000	Link
CVE-2023-21823	0.907830000	0.984380000	Link
CVE-2023-21554	0.902620000	0.983910000	Link
CVE-2023-20887	0.960660000	0.992630000	Link
CVE-2023-0669	0.965780000	0.994430000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 30 Aug 2023
[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Codeausführung
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 30 Aug 2023
[UPDATE] [hoch] Android Patchday Juli 2023
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 30 Aug 2023

[UPDATE] [hoch] vm2: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vm2 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 30 Aug 2023

[UPDATE] [kritisch] vm2: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vm2 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 30 Aug 2023

[UPDATE] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM Java ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 30 Aug 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, 30 Aug 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

—

Wed, 30 Aug 2023

[UPDATE] [hoch] Kubernetes: Mehrere Schwachstellen

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

- Link

—

Wed, 30 Aug 2023

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 30 Aug 2023

[NEU] [hoch] VMware Aria Operations for Networks: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in VMware Aria Operations for Networks ausnutzen, um Sicherheitsmaßnahmen zu umgehen und beliebigen Code auszuführen.

- Link

—

Wed, 30 Aug 2023

[NEU] [hoch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 30 Aug 2023

[NEU] [hoch] Aruba Switch: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Aruba Switch ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten, einen Denial-of-Service-Zustand zu verursachen und beliebigen Code

als privilegierter Benutzer auszuführen.
- Link
—
Wed, 30 Aug 2023
[NEU] [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
—
Tue, 29 Aug 2023
[NEU] [hoch] QEMU: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in QEMU ausnutzen, um seine Privilegien zu erhöhen, Code auszuführen oder einen Denial of Service zu verursachen.
- Link
—
Tue, 29 Aug 2023
[NEU] [UNGEPATCHT] [kritisch] yara: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in yara ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Tue, 29 Aug 2023
[NEU] [UNGEPATCHT] [hoch] Red Hat Ansible Automation Platform: Schwachstelle ermöglicht Manipulation von Dateien
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Ansible Automation Platform ausnutzen, um Dateien zu manipulieren.
- Link
—
Tue, 29 Aug 2023
[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link
—
Tue, 29 Aug 2023
[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.
- Link
—
Tue, 29 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um einen Denial of Service Angriff durchzuführen oder potenziell Code auszuführen.
- Link
—
Tue, 29 Aug 2023
[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/30/2023	[Ubuntu 20.04 LTS : Firefox vulnerabilities (USN-6320-1)]	critical
8/30/2023	[FreeBSD : chromium – use after free in MediaStream (22fffa69-46fa-11ee-8290-a8a1599412c6)]	critical
8/30/2023	[Security Update for Microsoft Visual Studio Code Concourse CI Pipeline Editor Extension (CVE-2022-31691)]	critical
8/30/2023	[Security Update for Microsoft Visual Studio Code Cloudfoundry Manifest YML Support Extension (CVE-2022-31691)]	critical
8/30/2023	[Security Update for Microsoft Visual Studio Code Bosh Editor Extension (CVE-2022-31691)]	critical
8/30/2023	[Security Update for Microsoft Visual Studio Code Spring Boot Tools Extension (CVE-2022-31691)]	critical
8/30/2023	[SUSE SLES12 Security Update : php7 (SUSE-SU-2023:3445-1)]	critical
8/30/2023	[SUSE SLES15 / openSUSE 15 Security Update : nodejs12 (SUSE-SU-2023:3455-1)]	critical
8/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : freetype2 (SUSE-SU-2023:3461-1)]	critical
8/30/2023	[SUSE SLES15 / openSUSE 15 Security Update : java-1_8_0-ibm (SUSE-SU-2023:3441-1)]	critical
8/30/2023	[Ubuntu 23.04 : Linux kernel vulnerabilities (USN-6321-1)]	high
8/30/2023	[openSUSE 15 Security Update : chromium (openSUSE-SU-2023:0237-1)]	high
8/30/2023	[Splunk Enterprise 8.2.0 < 8.2.12, 9.0.0 < 9.0.6, 9.1.0 < 9.1.1 (SVD-2023-0805)]	high
8/30/2023	[Splunk Enterprise 8.2.0 < 8.2.12, 9.0.0 < 9.0.6, 9.1.0 < 9.1.1 (SVD-2023-0806)]	high
8/30/2023	[Splunk Enterprise 8.2.0 < 8.2.12, 9.0.0 < 9.0.6, 9.1.0 < 9.1.1 (SVD-2023-0801)]	high
8/30/2023	[Splunk Enterprise 8.2.0 < 8.2.12, 9.0.0 < 9.0.6, 9.1.0 < 9.1.1 (SVD-2023-0804)]	high
8/30/2023	[Splunk Enterprise 8.2.0 < 8.2.12, 9.0.0 < 9.0.6, 9.1.0 < 9.1.1 (SVD-2023-0807)]	high
8/30/2023	[SUSE SLES12 Security Update : vim (SUSE-SU-2023:3463-1)]	high
8/30/2023	[SUSE SLES12 Security Update : clamav (SUSE-SU-2023:3435-1)]	high
8/30/2023	[SUSE SLES15 Security Update : qemu (SUSE-SU-2023:3444-1)]	high
8/30/2023	[SUSE SLES15 Security Update : ca-certificates-mozilla (SUSE-SU-2023:3462-1)]	high
8/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ca-certificates-mozilla (SUSE-SU-2023:3454-1)]	high
8/30/2023	[SUSE SLES15 / openSUSE 15 Security Update : haproxy (SUSE-SU-2023:3469-1)]	high
8/30/2023	[SUSE SLED12 / SLES12 Security Update : libcares2 (SUSE-SU-2023:3420-1)]	high
8/30/2023	[SUSE SLED15 / SLES15 Security Update : xen (SUSE-SU-2023:3447-1)]	high
8/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : webkit2gtk3 (SUSE-SU-2023:3419-1)]	high
8/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : clamav (SUSE-SU-2023:3456-1)]	high
8/30/2023	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2023-242-01)]	high
8/30/2023	[Slackware Linux 15.0 / current mozilla-thunderbird Vulnerability (SSA:2023-242-02)]	high
8/30/2023	[SUSE SLES15 Security Update : xen (SUSE-SU-2023:3446-1)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Wed, 30 Aug 2023
IQ-Medya CMS 2.0 Cross Site Scripting
IQ-Medya CMS version 2.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 30 Aug 2023
Apache NiFi H2 Connection String Remote Code Execution
The DBCPConnectionPool and HikariCPConnectionPool Controller Services in Apache NiFi 0.0.2 through 1.21.0 allow an authenticated and authorized user to configure a Database URL with the H2 driver that enables custom code execution. This exploit will result in several shells (5-7). Successfully tested against Apache nifi 1.17.0 through 1.21.0.
- Link
—
” “Wed, 30 Aug 2023
Juniper JunOS SRX / EX Remote Code Execution
A proof of concept exploit for chaining four CVEs to achieve remote code execution in Juniper JunOS within SRX and EX Series products.
- Link
—
” “Tue, 29 Aug 2023
Grawlix 1.5.1 Cross Site Scripting
Grawlix version 1.5.1 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 29 Aug 2023
GOM Player 2.3.90.5360 MITM / Remote Code Execution
GOM Player version 2.3.90.5360 man-in-the-middle proof of concept remote code execution exploit.
- Link
—
” “Tue, 29 Aug 2023
ImgHosting 1.2 Cross Site Scripting
ImgHosting version 1.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 29 Aug 2023
imax CMS 1.0 SQL Injection
imax CMS version 1.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Tue, 29 Aug 2023
i-Gallery 3.4 Database Disclosure
i-Gallery version 3.4 suffers from a database disclosure vulnerability.
- Link
—
” “Tue, 29 Aug 2023
iBilling CRM 4.5.0 Add Administrator / Insecure Direct Object Reference
iBilling CRM version 4.5.0 suffers from add administrator and insecure direct object reference vulnerabilities.
- Link
—
” “Tue, 29 Aug 2023
Humhub 1.3.13 Directory Traversal
Humhub version 1.3.13 suffers from a directory traversal vulnerability.
- Link
—
” “Tue, 29 Aug 2023
HumbertoCaldas CMS 0.1.3 Cross Site Scripting
HumbertoCaldas CMS version 0.1.3 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 29 Aug 2023

Human Resource PMS 1.4 Database Disclosure

Human Resource PMS version 1.4 suffers from a database disclosure vulnerability.

- Link

—

” “Tue, 29 Aug 2023

hudaallah Linker CMS 1.0 Cross Site Scripting

hudaallah Linker CMS version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 29 Aug 2023

HS-booking CMS 2.79 SQL Injection

HS-booking CMS version 2.79 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 29 Aug 2023

Foodiee Online Food Ordering Web Application 1.0.0 Cross Site Scripting

Foodiee Online Food Ordering Web Application version 1.0.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 29 Aug 2023

HRM SAAS 2.1.9 Insecure Settings

HRM SAAS version 2.1.9 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 29 Aug 2023

PHPValley Micro Jobs 2.0.1 Insecure Direct Object Reference

PHPValley Micro Jobs version 2.0.1 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Tue, 29 Aug 2023

Hloun 1.0.0 Insecure Settings

Hloun version 1.0.0 fails to remove the install script post installation allowing an unauthenticated user the ability to reinstall the system.

- Link

—

” “Tue, 29 Aug 2023

Hasan MWB 1 Add Administrator

Hasan MWB version 1 suffers from an add administrator vulnerability.

- Link

—

” “Tue, 29 Aug 2023

HPBoost 4.0 Add Administrator

HPBoost version 4.0 suffers from an add administrator vulnerability.

- Link

—

” “Mon, 28 Aug 2023

SPA-Cart eCommerce CMS 1.9.0.3 SQL Injection

SPA-Cart eCommerce CMS version 1.9.0.3 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 28 Aug 2023

SPA-Cart eCommerce CMS 1.9.0.3 Cross Site Scripting

SPA-Cart eCommerce CMS version 1.9.0.3 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 28 Aug 2023

Horse Market Sell And Rent Portal Script 1.5.7 Cross Site Scripting

Horse Market Sell and Rent Portal Script version 1.5.7 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 28 Aug 2023

Jorani 1.0.3 Cross Site Scripting

Jorani version 1.0.3 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 28 Aug 2023

HighPlus CMS 0.1.3 SQL Injection

HighPlus CMS version 0.1.3 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

”

0-Day

“Wed, 30 Aug 2023

ZDI-23-1286: Unified Automation UaGateway Certificate Parsing Integer Overflow Denial-of-Service Vulnerability

- Link

—

” “Wed, 30 Aug 2023

ZDI-23-1285: PaperCut NG External User Lookup Code Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 30 Aug 2023

ZDI-23-1284: NETGEAR ProSAFE Network Management System ZipUtils Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Wed, 30 Aug 2023

ZDI-23-1283: NETGEAR Orbi 760 SOAP API Authentication Bypass Vulnerability

- Link

—

” “Wed, 30 Aug 2023

ZDI-23-1282: Microsoft Teams Pluginhost Prototype Pollution Privilege Escalation Vulnerability

- Link

—

” “Tue, 29 Aug 2023

ZDI-23-1281: Apache ActiveMQ NMS Body Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

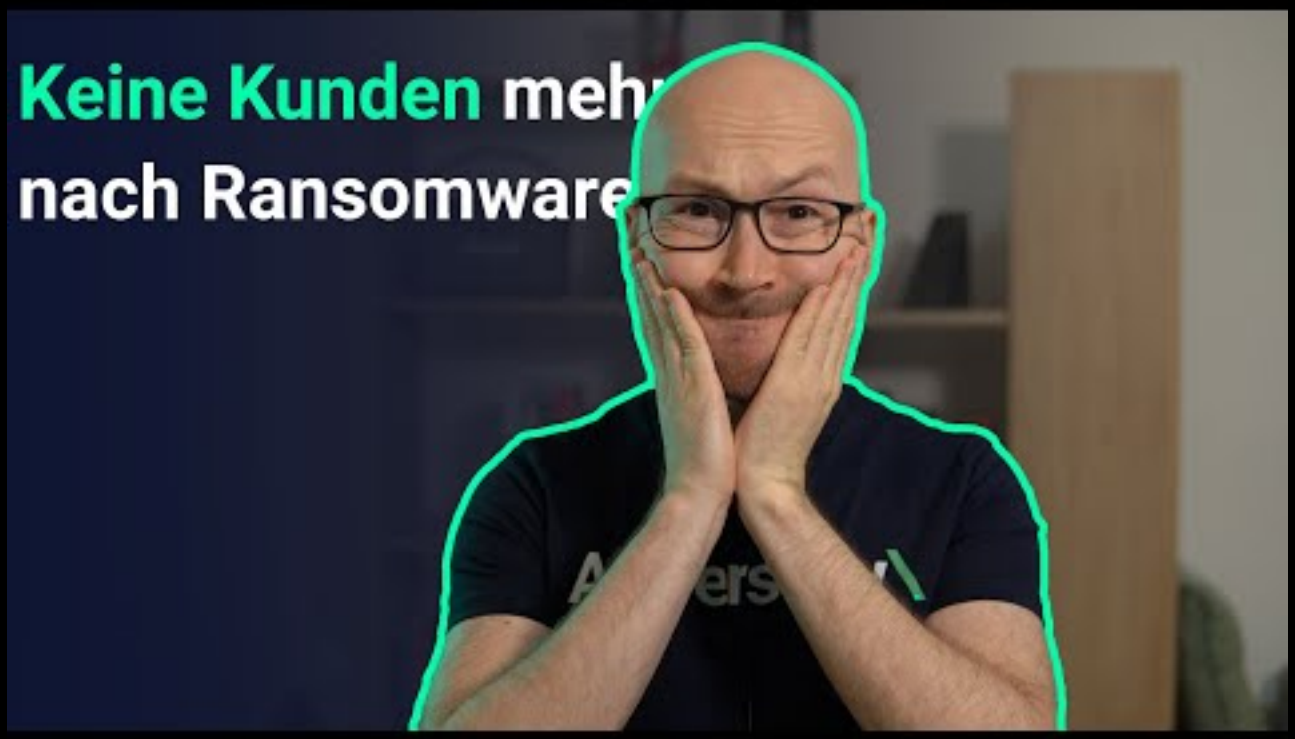
—

”

Die Hacks der Woche

mit Martin Haunschmid

“Ich glaube nicht, dass wir danach noch Kunden haben...”



Zum Youtube Video

Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2023-08-28	Kendrion	[NLD]	Link
2023-08-27	Hospital Sisters Health System (HSHS) et Prevea Health	[USA]	Link
2023-08-27	University of Michigan	[USA]	Link
2023-08-25	HTL Mödling	[AUT]	Link
2023-08-23	Haute École de Lucerne (HSLU)	[CHE]	Link
2023-08-23	Heuschen & Schrouff	[NLD]	Link
2023-08-22	Stadtbibliothek Weißwasser	[DEU]	Link
2023-08-22	Leaseweb	[NLD]	Link
2023-08-21	Hôpital municipal Sfânta Treime de Chișinău	[MDA]	Link
2023-08-21	Le Centre Public d'Action Sociale (CPAS) de Charleroi	[BEL]	Link
2023-08-21	St Helens Council	[GBR]	Link
2023-08-21	Hosteur	[CHE]	Link
2023-08-21	Carbon County	[USA]	Link
2023-08-20	Kansai Nerolac Ltd.	[IND]	Link
2023-08-20	Singing River Health System	[USA]	Link
2023-08-19	A1	[AUT]	Link
2023-08-18	Energy One Limited	[AUS]	Link
2023-08-18	AzeroCloud	[DNK]	Link
2023-08-17	Poste Italiane	[ITA]	Link
2023-08-17	La mairie de Sartrouville	[FRA]	Link
2023-08-16	Le consortium de bonification de l'Emilia Centrale	[ITA]	Link
2023-08-15	Cleveland City Schools	[USA]	Link
2023-08-14	Clorox	[USA]	Link
2023-08-14	Prince George's County Public Schools	[USA]	Link
2023-08-13	Swan Retail	[GBR]	Link
2023-08-13	Verlagsgruppe in München	[DEU]	Link
2023-08-12	Econocom	[FRA]	Link
2023-08-11	Neogy	[ITA]	Link
2023-08-11	Freeport-McMoRan Inc.	[USA]	Link
2023-08-09	Rapattoni	[USA]	Link
2023-08-08	Fondation de Verdeil	[CHE]	Link
2023-08-07	Centre médical Mayanei Hayeshua	[ISR]	Link
2023-08-07	Oniris	[FRA]	Link
2023-08-06	Le Service de Santé de Madeira (Sesaram)	[PRT]	Link
2023-08-04	Trinkwasserverband (TWV) Stader Land	[DEU]	Link
2023-08-03	Prospect Medical Holdings	[USA]	Link
2023-08-03	Commission des services électriques de Montréal (CSEM)	[CAN]	Link
2023-08-02	BPP	[GBR]	Link
2023-08-02	Joyson Safety Systems	[DEU]	Link
2023-08-02	L'Association du Barreau Fédéral Allemand (BRAK)	[DEU]	Link
2023-08-01	Programme de Soins Médicaux Intégrés (PAMI)	[ARG]	Link
2023-08-01	Eastern Connecticut Health Network (ECHN) et Waterbury HEALTH	[USA]	Link
2023-08-01	NOIRLab	[USA]	Link

Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-31	[antioch.edu]	lockbit3	Link
2023-08-31	[vitalitygroup.com]	clop	Link
2023-08-31	[zep.it]	lockbit3	Link
2023-08-31	[skystar.it]	lockbit3	Link
2023-08-31	[rydershealth.com]	lockbit3	Link
2023-08-30	[nieul-sur-mer.fr]	lockbit3	Link
2023-08-30	[tavlit.co.il]	lockbit3	Link
2023-08-30	[mariocoelho.com]	lockbit3	Link
2023-08-30	[grebe-korbach.de]	lockbit3	Link
2023-08-30	[optoflux.com]	lockbit3	Link
2023-08-30	[alpepipesystems.com]	lockbit3	Link
2023-08-30	[losh.com]	lockbit3	Link
2023-08-30	[greensboro.edu]	lockbit3	Link
2023-08-30	[emec.com.eg]	lockbit3	Link
2023-08-30	[auto-pieces.fr]	lockbit3	Link
2023-08-30	[guillerm-habitat.fr]	lockbit3	Link
2023-08-30	[acolea.org]	lockbit3	Link
2023-08-30	[otltd.co.uk]	lockbit3	Link
2023-08-30	[annals.edu.sg]	lockbit3	Link
2023-08-30	[inouemfg.com]	lockbit3	Link
2023-08-30	[potenciamaquinaria.com]	lockbit3	Link
2023-08-30	[locaparc.fr]	lockbit3	Link
2023-08-30	[dollinger-pierre.fr]	lockbit3	Link
2023-08-30	[feuille-erable.fr]	lockbit3	Link
2023-08-30	[texline-global.com]	lockbit3	Link
2023-08-30	[O'Brien Steel Service]	akira	Link
2023-08-30	[Aranui Cruises]	medusa	Link
2023-08-30	[Skynet]	medusa	Link
2023-08-30	[Renton School District]	akira	Link
2023-08-30	[Brooklyn Premier Orthopedics]	alphv	Link
2023-08-30	[lhvisionclinic.com]	lockbit3	Link
2023-08-30	[PRIDE GLOBAL CONSULTING SL]	8base	Link
2023-08-30	[Petkus Brothers]	8base	Link
2023-08-26	[Pasquale Bruni Ltd]	noescape	Link
2023-08-18	[Ningbo Yinzhou Vocational High School]	noescape	Link
2023-08-29	[sherwin-electric.com]	lockbit3	Link
2023-08-29	[beniculturali.it]	lockbit3	Link
2023-08-29	[jamaicainn.com]	lockbit3	Link
2023-08-29	[uprepschool.org]	lockbit3	Link
2023-08-29	[Zurvita]	ragroup	Link
2023-08-29	[casa-andina.com]	lockbit3	Link
2023-08-29	[renaultinantwerpen.be]	lockbit3	Link
2023-08-29	[greenside-sch.org]	lockbit3	Link
2023-08-29	[wkclawfirm.com]	lockbit3	Link
2023-08-29	[distribuidoradavidsa.com]	lockbit3	Link
2023-08-29	[cm.gov.nc.tr]	lockbit3	Link
2023-08-29	[younghomes.com]	lockbit3	Link
2023-08-29	[fimadev.fr]	lockbit3	Link
2023-08-29	[immoselekt.be]	lockbit3	Link
2023-08-29	[cloverbrook.com]	lockbit3	Link
2023-08-29	[carolfoxassociates.com]	lockbit3	Link
2023-08-29	[mergerecords.com]	lockbit3	Link
2023-08-29	[ukseung.co.kr]	lockbit3	Link
2023-08-29	[michalovich.co.il]	lockbit3	Link
2023-08-29	[Wright Moore DeHart Dupuis & Hutchinson]	alphv	Link
2023-08-29	[Forsyth County, GA]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-29	[esprigas.com]	lockbit3	Link
2023-08-29	[Agriloja pt.3]	everest	Link
2023-08-29	[PT. Cahaya Benteng Mas]	8base	Link
2023-08-29	[infinigate.ch]	clop	Link
2023-08-29	[Kendrion.com]	lockbit3	Link
2023-08-28	[PSM]	ransomed	Link
2023-08-28	[QI Holdings Ltd.]	noescape	Link
2023-08-23	[Iina Ba Inc]	noescape	Link
2023-08-28	[Asian Network Pacific Home Care & Hospice]	bianlian	Link
2023-08-28	[HealthIndia TPA Services Pvt Ltd]	bianlian	Link
2023-08-28	[Jasper High School]	akira	Link
2023-08-28	[Superior Communications]	alphv	Link
2023-08-28	[Intertek]	akira	Link
2023-08-28	[Penny Publications]	akira	Link
2023-08-28	[Voss Enterprises, Divvies]	akira	Link
2023-08-28	[Cutler-Smith]	akira	Link
2023-08-28	[GYP New Tree SA]	qilin	Link
2023-08-27	[grupomartex.com]	lockbit3	Link
2023-08-27	[jhilburn.com]	lockbit3	Link
2023-08-27	[Metropolitan Club DC]	ransomed	Link
2023-08-27	[Shanghai FRP Research Institute Co., Ltd.]	8base	Link
2023-08-27	[Fullerton India (SMFG India Credit)]	snatch	Link
2023-08-26	[State Farm]	ransomed	Link
2023-08-26	[Community Council of South Central Texas]	8base	Link
2023-08-26	[SKYROOT]	8base	Link
2023-08-26	[Varna Packaging]	8base	Link
2023-08-26	[KLM Laboratories Pvt. Ltd]	8base	Link
2023-08-21	[Gujarat Industries Power Company Ltd.]	noescape	Link
2023-08-22	[Alfagomma, Argus Fluidhandling Ltd]	play	Link
2023-08-25	[Trimaran Capital Partners]	alphv	Link
2023-08-25	[LEN Italia]	medusa	Link
2023-08-25	[Durham Fasteners]	medusa	Link
2023-08-25	[Axis Elevators]	medusa	Link
2023-08-25	[SMS-SME refused to protect customer and business data]	alphv	Link
2023-08-25	[Demcointer (Tunisia)]	alphv	Link
2023-08-25	[EPF]	alphv	Link
2023-08-25	[HFH Capital]	8base	Link
2023-08-25	[Prince George's County Public Schools]	rhysida	Link
2023-08-25	[SMS-SME was hacked. A huge amount of confidential information was stolen, information of c]	alphv	Link
2023-08-25	[Community Action]	8base	Link
2023-08-25	[INSTITUTO NACIONAL DE ELECTRIFICACION]	8base	Link
2023-08-25	[FA Foundry]	8base	Link
2023-08-25	[Sydenham Laboratories]	8base	Link
2023-08-18	[Fiocruz]	noescape	Link
2023-08-25	[senacrs.com.br]	lockbit3	Link
2023-08-24	[Edmonds School District]	akira	Link
2023-08-24	[Storm Tight Windows]	alphv	Link
2023-08-24	[Groupe Marchand Architecture & Design Inc]	alphv	Link
2023-08-24	[Bahamas Medical and Surgical Supplies]	8base	Link
2023-08-24	[Ontellus]	blackbyte	Link
2023-08-24	[Constellation Kidney Group]	bianlian	Link
2023-08-24	[Prospect Medical Holdings]	rhysida	Link
2023-08-24	[Arus-gmbh]	cloak	Link
2023-08-24	[Sportlab-srl]	cloak	Link
2023-08-24	[BONI-PASSAU.DE]	cloak	Link
2023-08-24	[lusis-avocats.com]	cloak	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-24	[werk33.com]	cloak	Link
2023-08-24	[GRIDINSTALLERS.com]	cloak	Link
2023-08-24	[surapon.com]	cloak	Link
2023-08-24	[mps-24.com]	cloak	Link
2023-08-24	[gruppomoba.com]	cloak	Link
2023-08-24	[stshcpa.com.tw]	cloak	Link
2023-08-24	[ihopmexico.com]	cloak	Link
2023-08-24	[Nicer technology]	cloak	Link
2023-08-24	[binhamoodah.ae]	cloak	Link
2023-08-24	[first-resources-ltd]	cloak	Link
2023-08-24	[Sbs-Berlin]	cloak	Link
2023-08-24	[imtmro.com]	cloak	Link
2023-08-24	[INCOBEC]	cloak	Link
2023-08-24	[still95.it]	cloak	Link
2023-08-24	[gsh-cargo.com]	cloak	Link
2023-08-24	[flamewarestudios.com]	cloak	Link
2023-08-24	[ALEZZELPOWER.com]	cloak	Link
2023-08-24	[Notaires.fr]	cloak	Link
2023-08-24	[Sonabhy.bf]	cloak	Link
2023-08-24	[KVFCU.ORG]	cloak	Link
2023-08-24	[Hoosick Falls Central School District]	8base	Link
2023-08-24	[Royal Oak Pet Clinic]	8base	Link
2023-08-24	[Mil-Ken Travel]	8base	Link
2023-08-24	[Kevills Solicitors]	8base	Link
2023-08-24	[The Law Offices of Steven H. Heisler]	8base	Link
2023-08-24	[Bahamas Medical & Surgical Supplies]	8base	Link
2023-08-23	[qintess.com]	lockbit3	Link
2023-08-23	[iledefrance-nature.fr]	lockbit3	Link
2023-08-23	[newsupri.com.br]	lockbit3	Link
2023-08-22	[IMS Computer Solutions]	alphv	Link
2023-08-23	[Transunion]	ransomed	Link
2023-08-23	[Jhookers]	ransomed	Link
2023-08-23	[Optimity]	ransomed	Link
2023-08-23	[Mambo]	stormous	Link
2023-08-23	[Nipun]	stormous	Link
2023-08-23	[Jasper]	stormous	Link
2023-08-23	[Econocom]	stormous	Link
2023-08-23	[digitalinsight.no]	clop	Link
2023-08-23	[mcnamaradrass.com]	lockbit3	Link
2023-08-23	[sti company]	arvinclub	Link
2023-08-22	[A???? F??????????? Ltd]	play	Link
2023-08-22	[tonystark.com]	lockbit3	Link
2023-08-22	[Sirius Computer Solutions]	alphv	Link
2023-08-22	[Atlantic Federal Credit Union]	alphv	Link
2023-08-22	[decrolyamericano.edu.gt]	lockbit3	Link
2023-08-22	[sicl.lk]	lockbit3	Link
2023-08-22	[NE-BIC]	alphv	Link
2023-08-22	[GROUPHC]	blackbasta	Link
2023-08-18	[Softverg Co., Ltd.]	noescape	Link
2023-08-13	[FYTISA Industrial Felts and FabricsSL]	noescape	Link
2023-08-13	[Infuance Communication Inc]	noescape	Link
2023-08-21	[Pierce College]	rhysida	Link
2023-08-21	[Department of Defence South African (DARPA)]	snatch	Link
2023-08-21	[apdparcel.com.au]	lockbit3	Link
2023-08-21	[TRIUNE TECHNOFAB PRIVATE LIMITED WAS HACKED]	alphv	Link
2023-08-21	[InG Brokers]	ransomed	Link
2023-08-21	[A1]	ransomed	Link
2023-08-21	[Department of Defence South African]	snatch	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-21	[Davidoff Hutcher & Citron]	alphv	Link
2023-08-21	[Seiko Group Corporation]	alphv	Link
2023-08-20	[stockwellharris.com]	lockbit3	Link
2023-08-20	[hallbergengineering.com]	lockbit3	Link
2023-08-20	[cloudtopoffice.com]	lockbit3	Link
2023-08-20	[equip-reuse.com]	lockbit3	Link
2023-08-20	[cochraninc.com]	lockbit3	Link
2023-08-19	[Novi Pazar put ad]	medusa	Link
2023-08-19	[The International Civil Defense Organization]	medusa	Link
2023-08-19	[Sartrouville France]	medusa	Link
2023-08-19	[goldmedalbakery]	cuba	Link
2023-08-19	[s3groupltd.com]	lockbit3	Link
2023-08-19	[macuspana.gob.mx]	lockbit3	Link
2023-08-19	[phitoformulas.com.br]	lockbit3	Link
2023-08-18	[ABS Auto Auctions]	play	Link
2023-08-18	[DSA Law Pty Ltd]	play	Link
2023-08-18	[Miami Management]	play	Link
2023-08-18	[BTC Power]	play	Link
2023-08-18	[Stanford Transportation Inc]	play	Link
2023-08-18	[Bolton Group]	play	Link
2023-08-18	[Legends Limousine]	play	Link
2023-08-18	[Oneonline]	play	Link
2023-08-18	[purever.com]	lockbit3	Link
2023-08-18	[neolife.com]	lockbit3	Link
2023-08-09	[mitchcointernational.com]	lockbit3	Link
2023-08-15	[tedpella.com]	lockbit3	Link
2023-08-11	[au Domain Administration Ltd]	noescape	Link
2023-08-11	[Contact 121 Pty Ltd]	noescape	Link
2023-08-17	[umchealth.com]	lockbit3	Link
2023-08-17	[sgl.co.th]	lockbit3	Link
2023-08-17	[Agriloja.pt demo-leak]	everest	Link
2023-08-17	[RIMSS]	akira	Link
2023-08-17	[SFJAZZ.ORG]	lockbit3	Link
2023-08-17	[mybps.us]	lockbit3	Link
2023-08-17	[kriegerklatt.com]	lockbit3	Link
2023-08-17	[ALLIANCE]	blackbasta	Link
2023-08-17	[DEUTSCHELEASING]	blackbasta	Link
2023-08-17	[VDVEN]	blackbasta	Link
2023-08-17	[SYNQUESTLABS]	blackbasta	Link
2023-08-17	[TWINTOWER]	blackbasta	Link
2023-08-17	[Camino Nuevo CharterAcademy]	akira	Link
2023-08-17	[Smart-swgcrc.org]	lockbit3	Link
2023-08-17	[The Clifton Public Schools]	akira	Link
2023-08-17	[MBO-PPS.COM]	clop	Link
2023-08-17	[MBOAMERICA.COM]	clop	Link
2023-08-17	[KOMORI.COM]	clop	Link
2023-08-16	[Dillon Supply]	metaencryptor	Link
2023-08-16	[Epicure]	metaencryptor	Link
2023-08-16	[Coswell]	metaencryptor	Link
2023-08-16	[BOB Automotive Group]	metaencryptor	Link
2023-08-16	[Seoul Semiconductor]	metaencryptor	Link
2023-08-16	[Kraiburg Austria GmbH]	metaencryptor	Link
2023-08-16	[Autohaus Ebert GmbH]	metaencryptor	Link
2023-08-16	[CVO Antwerpen]	metaencryptor	Link
2023-08-16	[ICON Creative Studio]	metaencryptor	Link
2023-08-16	[Heilmann Gruppe]	metaencryptor	Link
2023-08-16	[Schwälbchen Molkerei AG]	metaencryptor	Link
2023-08-16	[Münchner Verlagsgruppe GmbH]	metaencryptor	Link
2023-08-16	[Cequint]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-16	[Tally Energy Services]	akira	Link
2023-08-16	[CORDELLCORDELL]	alphv	Link
2023-08-16	[Municipality of Ferrara]	rhysida	Link
2023-08-16	[Hemmink]	incransom	Link
2023-08-16	[ToyotaLift Northeast]	8base	Link
2023-08-09	[FTRIA CO. LTD]	noescape	Link
2023-08-15	[Recaro]	alphv	Link
2023-08-15	[Postel SpA]	medusa	Link
2023-08-15	[ABA Research - Business Information 2]	alphv	Link
2023-08-15	[Keystone Insurance Services]	8base	Link
2023-08-15	[ANS]	8base	Link
2023-08-15	[Aspect Structural Engineers]	8base	Link
2023-08-08	[Fondation De Verdeil]	noescape	Link
2023-08-14	[Freeport-McMoran - NYSE: FCX]	alphv	Link
2023-08-14	[jhillburn.com]	lockbit3	Link
2023-08-14	[qbcqatar.com.qa]	lockbit3	Link
2023-08-07	[John L Lowery & Associates]	noescape	Link
2023-08-07	[Federal Bar Association]	noescape	Link
2023-08-14	[leecorpinc.com]	lockbit3	Link
2023-08-14	[econsult.com]	lockbit3	Link
2023-08-14	[Saint Xavier University]	alphv	Link
2023-08-14	[Agriloja.pt]	everest	Link
2023-08-14	[CB Energy Australlia]	medusa	Link
2023-08-14	[Borets (Levare.com)]	medusa	Link
2023-08-13	[majan.com]	lockbit3	Link
2023-08-13	[luterkort.se]	lockbit3	Link
2023-08-13	[difccourts.ae]	lockbit3	Link
2023-08-13	[zaun.co.uk]	lockbit3	Link
2023-08-13	[roxcel.com.tr]	lockbit3	Link
2023-08-13	[meaf.com]	lockbit3	Link
2023-08-13	[stmarysschool.co.za]	lockbit3	Link
2023-08-13	[rappenglitz.de]	lockbit3	Link
2023-08-13	[siampremier.co.th]	lockbit3	Link
2023-08-12	[National Institute of Social Services for Retirees and Pensioners]	rhysida	Link
2023-08-12	[Armortex]	bianlian	Link
2023-08-12	[arganoInterRel]	alphv	Link
2023-08-11	[Rite Technology]	akira	Link
2023-08-11	[zain.com]	lockbit3	Link
2023-08-10	[Top Light]	play	Link
2023-08-10	[Algorry Zappia & Associates]	play	Link
2023-08-10	[EAI]	play	Link
2023-08-10	[The Belt Railway Company of Chicago]	akira	Link
2023-08-10	[Optimum Technology]	akira	Link
2023-08-10	[Boson]	akira	Link
2023-08-10	[Stockdale Podiatry]	8base	Link
2023-08-09	[oneatlas.com]	lockbit3	Link
2023-08-05	[Lower Yukon School District]	noescape	Link
2023-08-06	[Thermenhotel Stoiser]	incransom	Link
2023-08-09	[el-cerrito.org]	lockbit3	Link
2023-08-09	[fashions-uk.com]	lockbit3	Link
2023-08-09	[cbcstjohns.co.za]	lockbit3	Link
2023-08-09	[octoso.de]	lockbit3	Link
2023-08-09	[ricks-motorcycles.com]	lockbit3	Link
2023-08-09	[janus-engineering.com]	lockbit3	Link
2023-08-09	[csem.qc.ca]	lockbit3	Link
2023-08-09	[asfcustomers.com]	lockbit3	Link
2023-08-09	[sekuro.com.tr]	lockbit3	Link
2023-08-09	[TIMECO]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-09	[chula.ac.th]	lockbit3	Link
2023-08-09	[etisaleg.com]	lockbit3	Link
2023-08-09	[2plan.com]	lockbit3	Link
2023-08-08	[Sabalan Azmayesh]	arvinclub	Link
2023-08-09	[Optimum Health Solutions]	rhysida	Link
2023-08-09	[unitycouncil.org]	lockbit3	Link
2023-08-09	[independenceia.org]	lockbit3	Link
2023-08-09	[www.finitia.net]	abyss	Link
2023-08-09	[Ramtha]	rhysida	Link
2023-08-08	[Batesville didn't react on appeal and allows Full Leak]	ragnarlocker	Link
2023-08-08	[ZESA Holdings]	everest	Link
2023-08-08	[Magic Micro Computers]	alphv	Link
2023-08-08	[Emerson School District]	medusa	Link
2023-08-08	[CH informatica]	8base	Link
2023-08-07	[Thonburi Energy Storage Systems (TESM)]	qilin	Link
2023-08-07	[Räddningstjänsten Västra Blekinge]	akira	Link
2023-08-07	[Papel Prensa SA]	akira	Link
2023-08-01	[Kreacta]	noescape	Link
2023-08-07	[Parsian Bitumen]	arvinclub	Link
2023-08-07	[varian.com]	lockbit3	Link
2023-08-06	[Delaney Browne Recruitment]	8base	Link
2023-08-06	[IBL]	alphv	Link
2023-08-05	[Draje food industrial group]	arvinclub	Link
2023-08-06	[Oregon Sports Medicine]	8base	Link
2023-08-06	[premierbpo.com]	alphv	Link
2023-08-06	[SatCom Marketing]	8base	Link
2023-08-05	[Rayden Solicitors]	alphv	Link
2023-08-05	[haynesintl.com]	lockbit3	Link
2023-08-05	[Kovair Software Data Leak]	everest	Link
2023-08-05	[Henlaw]	alphv	Link
2023-08-04	[mipe.com]	lockbit3	Link
2023-08-04	[armortex.com]	lockbit3	Link
2023-08-04	[iqcontrols.com]	lockbit3	Link
2023-08-04	[scottevest.com]	lockbit3	Link
2023-08-04	[atser.com]	lockbit3	Link
2023-08-04	[Galicia en Goles]	alphv	Link
2023-08-04	[tetco.com]	lockbit3	Link
2023-08-04	[SBS Construction]	alphv	Link
2023-08-04	[Koury Engineering]	akira	Link
2023-08-04	[Pharmatech Repblica Dominicana was hacked. All sensitive company and customer information]	alphv	Link
2023-08-04	[Grupo Garza Ponce was hacked! Due to a massive company vulnerability, more than 2 TB of se]	alphv	Link
2023-08-04	[seaside-kish co]	arvinclub	Link
2023-08-04	[Studio Domaine LLC]	nokoyawa	Link
2023-08-04	[THECHANGE]	alphv	Link
2023-08-04	[Ofimedic]	alphv	Link
2023-08-04	[Abatti Companies - Press Release]	monti	Link
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	Link
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	Link
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	Link
2023-08-03	[Venture General Agency]	akira	Link
2023-08-03	[Datawatch Systems]	akira	Link
2023-08-03	[admsc.com]	lockbit3	Link
2023-08-03	[United Tractors]	rhysida	Link
2023-08-03	[RevZero, Inc]	8base	Link
2023-08-03	[Rossman Realty Group, inc.]	8base	Link
2023-08-03	[riggsabney]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-02	[fec-corp.com]	lockbit3	Link
2023-08-02	[bestmotel.de]	lockbit3	Link
2023-08-02	[Tempur Sealy International]	alphv	Link
2023-08-02	[constructioncrd.com]	lockbit3	Link
2023-08-02	[Helen F. Dalton Lawyers]	alphv	Link
2023-08-02	[TGRWA]	akira	Link
2023-08-02	[Guido]	akira	Link
2023-08-02	[Bickel & Brewer - Press Release]	monti	Link
2023-08-02	[SHERMAN.EDU]	clop	Link
2023-08-02	[COSI]	karakurt	Link
2023-08-02	[unicorpusa.com]	lockbit3	Link
2023-08-01	[Garage Living, The Dispenser USA]	play	Link
2023-08-01	[Aapd]	play	Link
2023-08-01	[Birch, Horton, Bittner & Cherot]	play	Link
2023-08-01	[DAL-TECH Engineering]	play	Link
2023-08-01	[Coral Resort]	play	Link
2023-08-01	[Professionnel France]	play	Link
2023-08-01	[ACTIVA Group]	play	Link
2023-08-01	[Aquatlantis]	play	Link
2023-08-01	[Kogetsu]	mallox	Link
2023-08-01	[Parathon by JDA eHealth Systems]	akira	Link
2023-08-01	[KIMCO Staffing Service]	alphv	Link
2023-08-01	[Pea River Electric Cooperative]	nokoyawa	Link
2023-08-01	[MBS Equipment TTI]	8base	Link
2023-08-01	[gerb.bg]	lockbit3	Link
2023-08-01	[persingerlaw.com]	lockbit3	Link
2023-08-01	[Jacklett Construction LLC]	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.