



Ausgabe: 20230829

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

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](#)

Sicherheitsupdates: IBM Security Guardium auf mehreren Wegen angreifbar

IBM hat wichtige Sicherheitspatches für Security Guardium und Security Verify Access veröffentlicht.

- [Link](#)

Sicherheitslücken: Patches schützen Firewalls und Switches von Cisco

Angreifer können Geräte von Cisco via DoS-Attacken lahmlegen. Der Netzwerkausrüster hat Sicherheitspatches veröffentlicht.

- [Link](#)

WinRAR-Lücke weitreichender als gedacht

Am Wochenende wurde eine Sicherheitslücke in WinRAR bekannt. Die wirkt sich auf andere Software aus. Zudem gibt es weitere, bereits missbrauchte Lecks darin.

- [Link](#)

Asustor: Schwachstellen im NAS-Betriebssystem ermöglichen Übernahme

Das NAS-Betriebssystem Asustor Data Master enthält Sicherheitslücken, die Angreifern aus dem Netz die Übernahme ermöglichen. Ein Update ist verfügbar.

- [Link](#)

Schwachstellen im Web-Interface machen Aruba Orchestrator angreifbar

Angreifer können Arubas SD-WAN-Managementlösung EdgeConnect SD-WAN Orchestrator attackieren.

- [Link](#)

CISA warnt vor Angriffen auf Veeam-Backup-Sicherheitslücke

Die Cybersicherheitsbehörde CISA warnt vor aktuell laufenden Angriffen auf eine Veeam-Backup-Schwachstelle. Updates stehen bereit.

- [Link](#)

Webbrowser: Update für Google Chrome dichtet hochriskante Sicherheitslücken ab

Google hat den Webbrowser Chrome aktualisiert. Das Update dichtet fünf zum Teil als hochriskant eingestufte Lecks ab.

- [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	0.985620000	Link
CVE-2023-38035	0.918170000	0.985300000	Link
CVE-2023-3519	0.911990000	0.984740000	Link
CVE-2023-35078	0.965240000	0.994120000	Link
CVE-2023-34362	0.936790000	0.987700000	Link
CVE-2023-33246	0.963860000	0.993600000	Link
CVE-2023-32315	0.963250000	0.993420000	Link
CVE-2023-28771	0.917110000	0.985180000	Link
CVE-2023-28121	0.937820000	0.987800000	Link
CVE-2023-27372	0.970840000	0.996650000	Link
CVE-2023-27350	0.970350000	0.996380000	Link
CVE-2023-26360	0.908440000	0.984410000	Link
CVE-2023-25717	0.967140000	0.994960000	Link
CVE-2023-25194	0.924830000	0.985990000	Link
CVE-2023-24489	0.967300000	0.995040000	Link
CVE-2023-21839	0.961720000	0.992910000	Link
CVE-2023-21554	0.902620000	0.983930000	Link
CVE-2023-20887	0.960660000	0.992620000	Link
CVE-2023-0669	0.965780000	0.994400000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 28 Aug 2023

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

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

- [Link](#)

Mon, 28 Aug 2023

[NEU] [hoch] Notepad++: Mehrere Schwachstellen ermöglichen Codeausführung

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

- [Link](#)

Mon, 28 Aug 2023

[NEU] [hoch] Microsoft Edge: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Microsoft Edge ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Mon, 28 Aug 2023

[UPDATE] [hoch] win.rar WinRAR: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in win.rar WinRAR ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 28 Aug 2023

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

Ein entfernter anonymen Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

Fri, 25 Aug 2023

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR and Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

Fri, 25 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](#)

Fri, 25 Aug 2023

[UPDATE] [hoch] Xerox FreeFlow Print Server: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Print Server ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität des Systems zu gefährden.

- [Link](#)

Fri, 25 Aug 2023

[UPDATE] [kritisch] Ivanti Sentry: Schwachstelle ermöglicht Umgehung von Sicherheitsmechanismen

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Ivanti Sentry ausnutzen, um Sicherheitsmechanismen zu umgehen.

- [Link](#)

Fri, 25 Aug 2023

[UPDATE] [hoch] Kubernetes: Mehrere Schwachstellen

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

- [Link](#)

Fri, 25 Aug 2023

[NEU] [hoch] Verschiedene D-LINK Router und Access Point Modelle: Mehrere Schwachstellen

Ein entfernter anonymen Angreifer kann mehrere Schwachstellen in verschiedenen D-LINK Routern und Access Points ausnutzen, um die Netzwerkinfrastruktur anzugreifen, beliebigen Code auszuführen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Thu, 24 Aug 2023

[NEU] [hoch] binutils: Mehrere Schwachstellen

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in binutils ausnutzen, um einen Denial of

Service Angriff durchzuführen, Informationen offenzulegen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

Thu, 24 Aug 2023

[NEU] [hoch] IBM Security Guardium: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in IBM Security Guardium ausnutzen, um vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen oder beliebigen Code auszuführen.

- [Link](#)

Thu, 24 Aug 2023

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Offenlegung von Informationen

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

- [Link](#)

Thu, 24 Aug 2023

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Thu, 24 Aug 2023

[NEU] [hoch] Drupal Plugins: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in verschiedenen Drupal Plugins ausnutzen, um beliebigen Code auszuführen, sensible Informationen offenzulegen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Thu, 24 Aug 2023

[UPDATE] [hoch] OpenSSH: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in OpenSSH ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, seine Privilegien zu erweitern oder einen Denial of Service Angriff durchzuführen.

- [Link](#)

Thu, 24 Aug 2023

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

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

- [Link](#)

Thu, 24 Aug 2023

[UPDATE] [hoch] ImageMagick: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in ImageMagick ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Daten einzusehen oder weitere Angriffe mit nicht beschriebenen Auswirkungen durchzuführen.

- [Link](#)

Thu, 24 Aug 2023

[UPDATE] [hoch] ImageMagick: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in ImageMagick ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Daten einzusehen oder weitere Angriffe mit nicht beschriebenen Auswirkungen durchzuführen.

- [Link](#)

Datum	Schwachstelle	Bewertung
8/28/2023	[Ubuntu 22.04 LTS : json-c vulnerability (USN-6310-1)]	critical
8/28/2023	[Ubuntu 22.04 LTS / 23.04 : Libqb vulnerability (USN-6308-1)]	critical
8/25/2023	[Fedora 37 : GitPython (2023-26116901d9)]	critical
8/25/2023	[Rockwell Automation ThinManager ThinServer Path Traversal File Upload (CVE-2023-2917)]	critical
8/24/2023	[WinRAR < 6.23 RCE]	critical
8/24/2023	[Ubuntu 22.04 ESM : Fast DDS vulnerabilities (USN-6306-1)]	critical
8/24/2023	[Moxa (CVE-2023-4204)]	critical
8/28/2023	[Debian DLA-3544-1 : clamav - LTS security update]	high
8/28/2023	[Oracle Linux 8 : rust-toolset:ol8 (ELSA-2023-4635)]	high
8/28/2023	[FreeBSD : gitea – information disclosure (36a37c92-44b1-11ee-b091-6162c1274384)]	high
8/28/2023	[Rocky Linux 8 : postgresql:10 (RLSA-2023:4539)]	high
8/28/2023	[Rocky Linux 8 : subscription-manager (RLSA-2023:4706)]	high
8/28/2023	[Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-6309-1)]	high
8/27/2023	[Fedora 37 : clamav (2023-9f948bec13)]	high
8/27/2023	[Fedora 38 : caddy (2023-74e5545901)]	high
8/27/2023	[Fedora 37 : chromium (2023-5416cd3040)]	high
8/27/2023	[Fedora 37 : xen (2023-04473fc41e)]	high
8/27/2023	[Fedora 37 : caddy (2023-4926525509)]	high
8/27/2023	[Debian DLA-3542-1 : unrar-nonfree - LTS security update]	high
8/26/2023	[Microsoft Edge (Chromium) < 116.0.1938.62 Multiple Vulnerabilities]	high
8/26/2023	[Debian DSA-5483-1 : chromium - security update]	high
8/26/2023	[CBL Mariner 2.0 Security Update: qt5-qtbase (CVE-2023-37369)]	high
8/25/2023	[Fedora 38 : youtube-dl (2023-1f11546a48)]	high
8/25/2023	[Fedora 37 : youtube-dl (2023-5435c10480)]	high
8/25/2023	[Debian DSA-5482-1 : tryton-server - security update]	high
8/25/2023	[Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : JOSE for C/C++ vulnerability (USN-6307-1)]	high
8/25/2023	[Oracle Linux 9 : rust (ELSA-2023-4634)]	high
8/24/2023	[AlmaLinux 8 : subscription-manager (ALSA-2023:4706)]	high
8/24/2023	[Debian DLA-3541-1 : w3m - LTS security update]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“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](#)

” “Mon, 28 Aug 2023

Hospital HMS 2.7 SQL Injection

Hospital HMS version 2.7 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

” “Mon, 28 Aug 2023

Hospital HMS 2 SQL Injection

Hospital HMS version 2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

” “Mon, 28 Aug 2023

Hesk Rtl CMS 1 Cross Site Scripting

Hesk Rtl CMS version 1 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 28 Aug 2023

Hasan MWB 1 Cross Site Scripting

Hasan MWB version 1 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 28 Aug 2023

haraj 1.1 Add Administrator

haraj version 1.1 suffers from an add administrator vulnerability.

- [Link](#)

” “Mon, 28 Aug 2023

HaasCMS 1.0 Cross Site Scripting

HaasCMS version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 28 Aug 2023

Gusto Recipes Management 1.5.1 Cross Site Scripting

Gusto Recipes Management version 1.5.1 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 28 Aug 2023

Global Domains International 2.0 Cross Site Scripting

Global Domains International version 2.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 28 Aug 2023

FlightPath LMS 5.0-rc2 Cross Site Scripting

FlightPath LMS version 5.0-rc2 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

Business Directory Script 3.2 SQL Injection

Business Directory Script version 3.2 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

Gusto Recipes Management 1.5.1 Insecure Settings

Gusto Recipes Management version 1.5.1 suffers from an ignored default credential vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

Groupoffice 3.4.21 Directory Traversal

Groupoffice version 3.4.21 suffers from a directory traversal vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

Grawlix CMS 1.1.1 Cross Site Scripting

Grawlix CMS version 1.1.1 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

Gravira CMS 1.0 SQL Injection

Gravira CMS version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

Global Domains International 2.0 HTML Injection

Global Domains International version 2.0 suffers from an html injection vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

GetSimple CMS 3.3.2 Cross Site Scripting

GetSimple CMS version 3.3.2 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Fri, 25 Aug 2023

G And G Corporate CMS 1.0 SQL Injection

G and G Corporate CMS version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

” “Thu, 24 Aug 2023

Chamilo 1.11.18 Command Injection

This Metasploit module exploits an unauthenticated remote command execution vulnerability that affects Chamilo versions 1.11.18 and below. Due to a functionality called Chamilo Rapid to easily convert PowerPoint slides to courses on Chamilo, it is possible for an unauthenticated remote attacker to exe-

cute arbitrary commands at the OS level using a malicious SOAP request at the vulnerable endpoint /main/webservices/additional_webservices.php.

- [Link](#)

” “Thu, 24 Aug 2023

GEN Security+ 4.0 Cross Site Scripting

GEN Security+ version 4.0 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Thu, 24 Aug 2023

Geeklog 2.1.0b1 SQL Injection

Geeklog version 2.1.0b1 suffers from a remote SQL injection vulnerability.

- [Link](#)

”

0-Day

“Fri, 25 Aug 2023

ZDI-23-1280: D-Link DAP-2622 DDP Set SSID List Missing Authentication Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1279: D-Link DAP-2622 DDP Set Wireless Info Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1278: D-Link DAP-2622 DDP Set Wireless Info Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1277: D-Link DAP-2622 DDP Set SSID List PSK Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1276: D-Link DAP-2622 DDP Set SSID List RADIUS Server Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1275: D-Link DAP-2622 DDP Set SSID List RADIUS Secret Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1274: D-Link DAP-2622 DDP Set SSID List SSID Name Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1273: D-Link DAP-2622 DDP Set IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1272: D-Link DAP-2622 DDP Set IPv6 Address Secondary DNS Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1271: D-Link DAP-2622 DDP Set IPv6 Address Primary DNS Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1270: D-Link DAP-2622 DDP Set IPv6 Address Default Gateway Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1269: D-Link DAP-2622 DDP Set IPv6 Address Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1268: D-Link DAP-2622 DDP Set IPv6 Address Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1267: D-Link DAP-2622 DDP Set IPv4 Address Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1266: D-Link DAP-2622 DDP Set Device Info Device Name Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1265: D-Link DAP-2622 DDP Set Device Info Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1264: D-Link DAP-2622 DDP Set Device Info Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1263: D-Link DAP-2622 DDP Set Date-Time Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1262: D-Link DAP-2622 DDP Set Date-Time NTP Server Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1261: D-Link DAP-2622 DDP Set Date-Time Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1260: D-Link DAP-2622 DDP Set Date-Time Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1259: D-Link DAP-2622 DDP Set AG Profile NMS URL Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1258: D-Link DAP-2622 DDP Set AG Profile UUID Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1257: D-Link DAP-2622 DDP Set AG Profile Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1256: D-Link DAP-2622 DDP Set AG Profile Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1255: D-Link DAP-2622 DDP Get SSID List WPA PSK Information Disclosure Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1254: D-Link DAP-2622 DDP Firmware Upgrade Filename Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1253: D-Link DAP-2622 DDP Firmware Upgrade Server IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1252: D-Link DAP-2622 DDP Firmware Upgrade Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1251: D-Link DAP-2622 DDP Firmware Upgrade Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1250: D-Link DAP-2622 DDP Configuration Restore Filename Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1249: D-Link DAP-2622 DDP Configuration Restore Server IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1248: D-Link DAP-2622 DDP Configuration Restore Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1247: D-Link DAP-2622 DDP Configuration Restore Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1246: D-Link DAP-2622 DDP Configuration Backup Filename Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1245: D-Link DAP-2622 DDP Configuration Backup Server Address Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1244: D-Link DAP-2622 DDP Configuration Backup Server IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1243: D-Link DAP-2622 DDP Configuration Backup Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1242: D-Link DAP-2622 DDP Configuration Backup Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1241: D-Link DAP-2622 DDP Change ID Password New Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1240: D-Link DAP-2622 DDP Change ID Password New Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1239: D-Link DAP-2622 DDP Change ID Password Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1238: D-Link DAP-2622 DDP Reset Factory Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1237: D-Link DAP-2622 DDP Reset Factory Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1236: D-Link DAP-2622 DDP Reset Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1235: D-Link DAP-2622 DDP Reset Auth Username Stack-based Buffer Overflow Re-

mote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1234: D-Link DAP-2622 DDP Reboot Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1233: D-Link DAP-2622 DDP Reboot Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1232: D-Link DAP-2622 DDP User Verification Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1231: D-Link DAP-2622 DDP User Verification Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1230: D-Link DAP-2622 Telnet CLI Use of Hardcoded Credentials Authentication Bypass Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1229: Adobe Dimension USD File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1228: Samba Spotlight mdssvc RPC Request Type Confusion Information Disclosure Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1227: Samba Spotlight mdssvc RPC Request Infinite Loop Denial-of-Service Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1226: Apple macOS ImageIO EXR File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1225: Apple macOS EXR Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1224: LG LED Assistant updateFile Directory Traversal Information Disclosure Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1223: LG LED Assistant thumbnail Directory Traversal Information Disclosure Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1222: LG LED Assistant setThumbnailRc Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

” “Fri, 25 Aug 2023

ZDI-23-1221: LG LED Assistant upload Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

”

Die Hacks der Woche

mit Martin Haunschmid

Wasser predigen und Wein trinken? Ivanti, als Security Hersteller DARF so etwas nicht passieren!



[Zum Youtube Video](#)

Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
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 Chişinău	[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-Gruppe	Webseite
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	[luis-avocats.com]	cloak	Link
2023-08-24	[werk33.com]	cloak	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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]	clon	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	[decoyamericano.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
2023-08-21	[Davidoff Hutter & Citron]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[s3group ltd.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-swgcr.org]	lockbit3	Link
2023-08-17	[The Clifton Public Schools]	akira	Link
2023-08-17	[MBO-PPS.COM]	clon	Link
2023-08-17	[MBOAMERICA.COM]	clon	Link
2023-08-17	[KOMORI.COM]	clon	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	[Cequent]	akira	Link
2023-08-16	[Tally Energy Services]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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
2023-08-09	[chula.ac.th]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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
2023-08-02	[fec-corp.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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]	cl0p	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.