Cybersecurity Morgenreport

Ausgabe: 20230824

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

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: Smarte Glühbirne von TP-Link als Einfallstor ins WLAN
Sicherheitsforscher warnen in einem wissenschaftlichen Artikel welche Gefahr selbst von vergleichsweise simplen IoT-Geräten ausgehen kann.
- Link

—

Jetzt patchen! Angreifer schieben Schadcode durch Lücke in Adobe ColdFusion
Angreifer attackieren Adobes Middleware ColdFusion. Sicherheitsupdates sind verfügbar.
- Link

—

Kritische Sicherheitslücke in Ivanti Sentry wird bereits missbraucht
Ivanti schließt in Sentry, vormals MobileIron Sentry, eine kritische Sicherheitslücke. Sie wird bereits angegriffen.
- Link

—

Angreifer können Sicherheitslücken in Junos OS zu kritischer Gefahr eskalieren
Das Netzwerkbetriebssystem Junos OS ist über mehrere Schwachstellen attackierbar. Dagegen abgesicherte Versionen stehen zum Download bereit.
- Link

—

Update bereits ausgespielt: Kritische Lücke in WinRAR erlaubte Code-Ausführung
Das verbreitete Kompressionstool WinRAR besaß in älteren Versionen eine schwere Lücke, die beliebige Codeausführung erlaubte. Die aktuelle Version schließt sie.
- Link

—

Sicherheitslösung: IBM Security Guardium als Einfallstor für Angreifer
Eine kritische Lücke bedroht Systeme mit IBM Security Guardium. Sicherheitspatches sind verfügbar.
- 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	0.985600000	Link
CVE-2023-3519	0.911990000	0.984750000	Link
CVE-2023-35078	0.965240000	0.994130000	Link
CVE-2023-34362	0.936790000	0.987670000	Link
CVE-2023-33246	0.963860000	0.993570000	Link
CVE-2023-28771	0.918810000	0.985360000	Link
CVE-2023-28121	0.937820000	0.987770000	Link
CVE-2023-27372	0.970840000	0.996620000	Link
CVE-2023-27350	0.970350000	0.996360000	Link
CVE-2023-25717	0.967140000	0.994970000	Link
CVE-2023-25194	0.924830000	0.985950000	Link
CVE-2023-24489	0.967300000	0.995040000	Link
CVE-2023-21839	0.961530000	0.992850000	Link
CVE-2023-21554	0.902620000	0.983900000	Link
CVE-2023-20887	0.960660000	0.992620000	Link
CVE-2023-0669	0.965780000	0.994390000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 23 Aug 2023
[NEU] [hoch] Aruba EdgeConnect SD-WAN Orchestrator: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Aruba EdgeConnect SD-WAN Orchestrator ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Informationen offenzulegen und zu manipulieren und um die Kontrolle über das System zu übernehmen.
- Link

Wed, 23 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, 23 Aug 2023
[NEU] [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

—

Wed, 23 Aug 2023
[NEU] [hoch] BusyBox: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle in BusyBox ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 23 Aug 2023
[NEU] [UNGEPATCHT] [kritisch] Perl: Schwachstelle ermöglicht Privilegieneskalation
Ein Angreifer kann eine Schwachstelle in Perl ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Wed, 23 Aug 2023
[NEU] [hoch] IBM Spectrum Protect: Mehrere Schwachstellen
Ein lokaler oder entfernter Angreifer kann mehrere Schwachstellen in IBM Spectrum Protect ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen, einen Denial of Service Zustand herbeizuführen oder unbekannte Auswirkungen zu verursachen.
- Link

—

Wed, 23 Aug 2023
[NEU] [hoch] Google Chrome: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.
- Link

—

Wed, 23 Aug 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.
- Link

—

Wed, 23 Aug 2023
[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Wed, 23 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, 23 Aug 2023
[UPDATE] [hoch] Intel Firmware: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in der Intel Firmware und dem Intel Chipsatz ausnutzen, um seine Privilegien zu erhöhen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Wed, 23 Aug 2023
[UPDATE] [kritisch] Ivanti Sentry: Schwachstelle ermöglicht Umgehung von Sicherheitsmechanismen
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ivanti Sentry ausnutzen, um Sicherheitsmechanismen zu umgehen.
- Link

—

Tue, 22 Aug 2023
[UPDATE] [kritisch] Python: Schwachstelle ermöglicht Codeausführung
Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Tue, 22 Aug 2023
[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link
—
Tue, 22 Aug 2023
[UPDATE] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 21 Aug 2023
[NEU] [hoch] Moodle: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um Sicherheitsmechanismen zu umgehen, Informationen offenzulegen und SQL-Injection- oder Cross-Site-Scripting-Angriffe durchzuführen.
- Link
—
Mon, 21 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-Zustand herbeizuführen, Speicher zu verändern und möglicherweise beliebigen Code auszuführen.
- Link
—
Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und einen nicht spezifizierten Angriff durchzuführen.
- Link
—
Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Mon, 21 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/23/2023	[Dell Cyber Recovery < 19.11.0.2 Authentication Bypass (DSA-2022-196)]	critical
8/23/2023	[Amazon Linux 2 : log4j (ALAS-2022-1739)]	critical
8/23/2023	[Amazon Linux AMI : php71-pecl-imagick (ALAS-2023-1814)]	critical
8/23/2023	[Amazon Linux AMI : openssh (ALAS-2023-1802)]	critical

Datum	Schwachstelle	Bewertung
8/23/2023	[Amazon Linux AMI : php55-pecl-imagick (ALAS-2023-1812)]	critical
8/23/2023	[Amazon Linux AMI : php54-pecl-imagick (ALAS-2023-1810)]	critical
8/23/2023	[Amazon Linux 2 : oniguruma (ALAS-2023-2217)]	critical
8/23/2023	[Amazon Linux AMI : php56-pecl-imagick (ALAS-2023-1811)]	critical
8/23/2023	[Amazon Linux AMI : php70-pecl-imagick (ALAS-2023-1813)]	critical
8/23/2023	[Amazon Linux 2 : containerd (ALASDOCKER-2023-029)]	critical
8/23/2023	[Amazon Linux AMI : php72-pecl-imagick (ALAS-2023-1815)]	critical
8/23/2023	[Debian DLA-3540-1 : mediawiki - LTS security update]	critical
8/23/2023	[FreeBSD : phpmyfaq – multiple vulnerabilities (ddd3fcc9-2bdd-11ee-9af4-589cfc0f81b0)]	high
8/23/2023	[Amazon Linux AMI : monit (ALAS-2023-1805)]	high
8/23/2023	[Amazon Linux 2 : kernel (ALAS-2023-2206)]	high
8/23/2023	[Amazon Linux AMI : kernel (ALAS-2023-1803)]	high
8/23/2023	[Amazon Linux 2 : exiv2 (ALAS-2023-2215)]	high
8/23/2023	[Amazon Linux AMI : openldap (ALAS-2023-1804)]	high
8/23/2023	[Amazon Linux AMI : GraphicsMagick (ALAS-2023-1806)]	high
8/23/2023	[AlmaLinux 9 : subscription-manager (ALSA-2023:4708)]	high
8/23/2023	[Amazon Linux 2 : glibc (ALAS-2023-2221)]	high
8/23/2023	[Amazon Linux AMI : amanda (ALAS-2023-1808)]	high
8/23/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2023-051)]	high
8/23/2023	[Amazon Linux 2 : spice-protocol (ALAS-2023-2219)]	high
8/23/2023	[Amazon Linux 2 : libgovirt (ALAS-2023-2220)]	high
8/23/2023	[Amazon Linux 2 : amanda (ALAS-2023-2218)]	high
8/23/2023	[Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2023-1809)]	high
8/23/2023	[Wireshark 4.0.x < 4.0.8 Multiple Vulnerabilities]	high
8/23/2023	[Wireshark 4.0.x < 4.0.8 Multiple Vulnerabilities (macOS)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Wed, 23 Aug 2023
CrafterCMS 4.0.2 Cross Site Scripting
CrafterCMS versions 4.0.2 and below suffer from multiple cross site scripting vulnerabilities.
- Link
—
” “Wed, 23 Aug 2023
SugarCRM 12.2.0 SQL Injection
SugarCRM versions 12.2.0 and below suffer from multiple remote SQL injection vulnerabilities.
- Link
—
” “Wed, 23 Aug 2023
SugarCRM 12.2.0 PHP Object Injection
SugarCRM versions 12.2.0 and below suffer from a PHP object injection vulnerability.
- Link
—
” “Wed, 23 Aug 2023
SugarCRM 12.2.0 Bean Manipulation
SugarCRM versions 12.2.0 suffer from a bean manipulation vulnerability that can allow for privilege escalation.
- Link
—
” “Wed, 23 Aug 2023
SugarCRM 12.2.0 Shell Upload
SugarCRM versions 12.2.0 and below suffers from a multiple step remote shell upload vulnerability.
- Link
—
” “Wed, 23 Aug 2023
GEN Security+ 4.0 SQL Injection
GEN Security+ version 4.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Wed, 23 Aug 2023
Geeklog 2.1.0b1 Database Disclosure
Geeklog version 2.1.0b1 suffers from a database disclosure vulnerability.
- Link
—
” “Wed, 23 Aug 2023
G And G Corporate CMS 1.0 Cross Site Scripting
G and G Corporate CMS version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 23 Aug 2023
FreshRSS 1.11.1 HTML Injection
FreshRSS version 1.11.1 suffers from an html injection vulnerability.
- Link
—
” “Wed, 23 Aug 2023
Forum Fire Soft Board 0.3.0 Cross Site Scripting
Forum Fire Soft Board version 0.3.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 23 Aug 2023
Forma LMS 1.4 Database Disclosure
Forma LMS version 1.4 suffers from a database disclosure vulnerability.
- Link
—
” “Wed, 23 Aug 2023
Foodiee CMS 1.0.1 Insecure Direct Object Reference

Foodiee CMS version 1.0.1 suffers from an insecure direct object reference vulnerability.
- Link
—
” “Wed, 23 Aug 2023
Foodiee Online Food Ordering Web Application 1.0.0 Insecure Settings
Foodiee Online Food Ordering Web Application version 1.0.0 suffers from an ignored default credential vulnerability.
- Link
—
” “Wed, 23 Aug 2023
FlightPath LMS 4.8.2 Cross Site Scripting
FlightPath LMS version 4.8.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Wed, 23 Aug 2023
FixBook Repair Shop Management Tool 3.0 Hash Disclosure
FixBook Repair Shop Management Tool version 3.0 suffers from an information leakage vulnerability.
- Link
—
” “Wed, 23 Aug 2023
FAST TECH CMS 1.0 SQL Injection
FAST TECH CMS version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Tue, 22 Aug 2023
WordPress Charitable Donations Plugin And Fundraising Platform 1.7.0.12 Privilege Escalation
WordPress Charitable Donations Plugin and Fundraising Platform versions 1.7.0.12 and below suffer from a privilege escalation vulnerability.
- Link
—
” “Tue, 22 Aug 2023
TSPlus 16.0.2.14 Insecure Permissions
TSPlus version 16.0.2.14 suffers from an insecure permissions vulnerability.
- Link
—
” “Tue, 22 Aug 2023
TSPlus 16.0.0.0 Insecure Permissions
TSPlus version 16.0.0.0 suffers from an insecure permissions vulnerability.
- Link
—
” “Tue, 22 Aug 2023
TSPlus 16.0.0.0 Insecure Credential Storage
TSPlus version 16.0.0.0 suffers from an insecure credential storage vulnerability.
- Link
—
” “Tue, 22 Aug 2023
Inosoft VisiWin 7 2022-2.1 Insecure Permissions / Privilege Escalation
Inosoft VisiWin 7 version 2022-2.1 suffers from a privilege escalation vulnerability.
- Link
—
” “Tue, 22 Aug 2023
Dolibarr 17.0.1 Cross Site Scripting
Dolibarr version 17.0.1 suffers from a persistent cross site scripting vulnerability.
- Link
—
” “Tue, 22 Aug 2023
PHPJabbers Business Directory Script 3.2 Cross Site Request Forgery / Cross Site Scripting
PHPJabbers Business Directory Script version 3.2 suffers from cross site request forgery and cross site scripting vulnerabilities.
- Link

—
” “Tue, 22 Aug 2023
FOG Forum 0.8 Cross Site Scripting
FOG Forum version 0.8 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 22 Aug 2023
FoccusWeb CMS 0.1 Cross Site Scripting
FoccusWeb CMS version 0.1 suffers from a cross site scripting vulnerability.
- Link
—
”

0-Day

“Wed, 23 Aug 2023
ZDI-23-1168: Zabbix Web Service Report Generation External Control of File Name Information Disclosure Vulnerability
- Link
—
” “Wed, 23 Aug 2023
ZDI-23-1167: Ivanti Avalanche decodeToMap XML External Entity Processing Information Disclosure Vulnerability
- Link
—
” “Wed, 23 Aug 2023
ZDI-23-1166: ASUS RT-AX92U lighttpd mod_webdav.so SQL Injection Information Disclosure Vulnerability
- Link
—
” “Wed, 23 Aug 2023
ZDI-23-1165: 7-Zip 7Z File Parsing Integer Underflow Remote Code Execution Vulnerability
- Link
—
” “Wed, 23 Aug 2023
ZDI-23-1164: 7-Zip SquashFS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Tue, 22 Aug 2023
ZDI-23-1163: NETGEAR RAX30 Telnet CLI passwd Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Tue, 22 Aug 2023
ZDI-23-1162: NETGEAR RAX30 DHCP Server Command Injection Remote Code Execution Vulnerability
- Link
—
” “Tue, 22 Aug 2023
ZDI-23-1161: NETGEAR RAX30 UPnP Command Injection Remote Code Execution Vulnerability
- Link
—
” “Tue, 22 Aug 2023
ZDI-23-1160: Parse Server transformUpdate Prototype Pollution Remote Code Execution Vulnerability
- Link
—
” “Tue, 22 Aug 2023
ZDI-23-1159: Apple macOS KTX Image Parsing Out-Of-Bounds Read Information Disclosure

Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1158: McAfee Safe Connect VPN Uncontrolled Search Path Element Local Privilege Escalation Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1157: Advantech R-SeeNet device_status Local File Inclusion Privilege Escalation Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1156: Advantech R-SeeNet Use Of Hard-Coded Credentials Authentication Bypass Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1155: SonicWALL GMS Virtual Appliance HttpDigestAuthenticator Authentication Bypass Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1154: SonicWALL GMS Virtual Appliance Syslog Directory Traversal Remote Code Execution Vulnerability
- Link
—
” “Mon, 21 Aug 2023
ZDI-23-1153: 3CX Uncontrolled Search Path Local Privilege Escalation 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
2023-08-22	Stadtbibliothek Weißwasser	[DEU]	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	[FRA]	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
2023-08-23	[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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.