
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240229



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	7
3.3 Sicherheitslücken Meldungen von Tenable	10
4 Aktiv ausgenutzte Sicherheitslücken	13
4.1 Exploits der letzten 5 Tage	13
4.2 0-Days der letzten 5 Tage	17
5 Die Hacks der Woche	19
5.0.1 EXTRABLATT: Lockbit down? UND: ScreenConnect-Lücke (10/10 kritisch) . . .	19
6 Cyberangriffe: (Feb)	20
7 Ransomware-Erpressungen: (Feb)	22
8 Quellen	36
8.1 Quellenverzeichnis	36
9 Impressum	37

1 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

2 Security-News

2.1 Heise - Security-Alert

Teamviewer: Sicherheitslücke im Client ermöglicht Rechteausweitung

Eine Schwachstelle im Teamviewer-Client ermöglicht Nutzern, ihre Rechte im System auszuweiten. Ein Update steht bereit.

- [Link](#)

—

Google Chrome: Sicherheitsupdate bessert vier Schwachstellen aus

Googles Entwickler haben den Webbrowser Chrome in neuer Version veröffentlicht. Sie schließen damit vier Sicherheitslücken.

- [Link](#)

—

Remote-Desktop: RustDesk-Update entfernt Test-Zertifikat

Ein Test-Zertifikat in RustDesk für Windows führte zu Diskussionen. Ein Update entfernt es, mitsamt einiger Funktionen.

- [Link](#)

—

Webbrowser: Microsoft Edge-Update schließt Sicherheitslücken

Microsoft hat am Freitag den Browser Edge aktualisiert. Neben Chromium-Sicherheitslücken dichten die Entwickler auch eigene ab.

- [Link](#)

—

Kritische Lücke in Wordpress-Plug-in Ultimate Member leakt Passwort-Hashes

Angreifer können Wordpress-Websites mit dem Plug-in Ultimate Member attackieren. Potenziell sind mehr als 200.000 Seiten gefährdet.

- [Link](#)

—

WS_FTP: Updates dichten hochriskante Sicherheitslücke ab

In WS-FTP von Progress klafft eine Sicherheitslücke, die Angreifern Cross-Site-Scripting-Angriffe ermöglicht. Ein Update steht bereit.

- [Link](#)

—

Sicherheitslücken: GitLab gegen mögliche Attacken abgesichert

Updates schließen mehrere Schwachstellen in GitLab. Eine Lücke bleibt aber offensichtlich erstmal bestehen.

- [Link](#)

Sicherheitsupdate: Root-Lücke bedroht Servermonitoringtool Nagios XI

Admins sollten das Dienste-Monitoring mit Nagios XI aus Sicherheitsgründen zeitnah auf den aktuellen Stand bringen.

- [Link](#)

CMS Joomla bessert riskante Schwachstellen aus

Das Joomla-Projekt schließt mit den Versionen 5.0.3 und 4.4.3 Sicherheitslücken. Angreifer können dadurch etwa Dateien manipulieren.

- [Link](#)

HP Laser-Drucker: Sicherheitslücken erlauben Codeschmuggel

HP warnt mit gleich zwei Sicherheitsmeldungen vor Lücken in diversen Laserjet-Druckern. Firmware-updates sollen sie schließen.

- [Link](#)

3 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.

3.1 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.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-6553	0.916210000	0.988220000	Link
CVE-2023-5360	0.967230000	0.996320000	Link
CVE-2023-4966	0.963970000	0.995230000	Link
CVE-2023-47246	0.943540000	0.991320000	Link
CVE-2023-46805	0.962740000	0.994840000	Link
CVE-2023-46747	0.972020000	0.998000000	Link
CVE-2023-46604	0.972850000	0.998440000	Link
CVE-2023-43177	0.932620000	0.990010000	Link
CVE-2023-42793	0.972940000	0.998510000	Link
CVE-2023-41265	0.915100000	0.988070000	Link
CVE-2023-39143	0.925430000	0.989210000	Link
CVE-2023-38646	0.904440000	0.987190000	Link
CVE-2023-38205	0.934710000	0.990200000	Link
CVE-2023-38203	0.949400000	0.992210000	Link
CVE-2023-38035	0.974160000	0.999250000	Link
CVE-2023-36845	0.965590000	0.995790000	Link
CVE-2023-3519	0.908750000	0.987590000	Link
CVE-2023-35082	0.934310000	0.990160000	Link
CVE-2023-35078	0.949930000	0.992280000	Link
CVE-2023-34960	0.925010000	0.989190000	Link
CVE-2023-34634	0.919000000	0.988500000	Link
CVE-2023-34362	0.959040000	0.993990000	Link
CVE-2023-3368	0.928930000	0.989550000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-33246	0.973410000	0.998770000	Link
CVE-2023-32315	0.973960000	0.999100000	Link
CVE-2023-32235	0.902020000	0.987080000	Link
CVE-2023-30625	0.951530000	0.992550000	Link
CVE-2023-30013	0.936180000	0.990350000	Link
CVE-2023-29300	0.963530000	0.995100000	Link
CVE-2023-29298	0.921360000	0.988730000	Link
CVE-2023-28771	0.923800000	0.989050000	Link
CVE-2023-28121	0.933120000	0.990070000	Link
CVE-2023-27524	0.972330000	0.998220000	Link
CVE-2023-27372	0.971580000	0.997800000	Link
CVE-2023-27350	0.972270000	0.998190000	Link
CVE-2023-26469	0.946560000	0.991750000	Link
CVE-2023-26360	0.960730000	0.994410000	Link
CVE-2023-26035	0.969370000	0.996970000	Link
CVE-2023-25717	0.962180000	0.994690000	Link
CVE-2023-2479	0.963310000	0.995040000	Link
CVE-2023-24489	0.973430000	0.998800000	Link
CVE-2023-23752	0.948570000	0.992110000	Link
CVE-2023-23397	0.917330000	0.988330000	Link
CVE-2023-22527	0.965680000	0.995830000	Link
CVE-2023-22518	0.969180000	0.996910000	Link
CVE-2023-22515	0.973330000	0.998730000	Link
CVE-2023-21839	0.962110000	0.994670000	Link
CVE-2023-21554	0.961220000	0.994480000	Link
CVE-2023-20887	0.965640000	0.995810000	Link
CVE-2023-20198	0.919220000	0.988520000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-1671	0.964250000	0.995320000	Link
CVE-2023-0669	0.968020000	0.996570000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 28 Feb 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in Oracle Linux ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Microsoft Azure Site Recovery und Azure Storage: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Azure Site Recovery und Azure Storage ausnutzen, um seine Privilegien zu erhöhen, Informationen offenzulegen oder beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[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, 28 Feb 2024

[UPDATE] [hoch] Intel i915 Graphics Driver für Linux: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Intel i915 Graphics Driver für Linux ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Linux Kernel (vmwgfx): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

Wed, 28 Feb 2024

[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Wed, 28 Feb 2024

[NEU] [hoch] tribe29 checkmk: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in tribe29 checkmk ausnutzen, um beliebigen Programmcode auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 28 Feb 2024

[NEU] [hoch] Arista EOS: Schwachstelle ermöglicht Codeausführung

Ein entfernter authentifizierter Angreifer kann eine Schwachstelle in Arista EOS ausnutzen, um beliebigen Code auszuführen.

- [Link](#)

—

Tue, 27 Feb 2024

[UPDATE] [hoch] cobbler: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in cobbler ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/28/2024	[Fedora 38 : yarnpkg (2024-5ecc250449)]	critical
2/28/2024	[Fedora 39 : yarnpkg (2024-28fc0c2ef4)]	critical

Datum	Schwachstelle	Bewertung
2/28/2024	[Fortinet FortiProxy Out-of-bound Write in sslvpnd (FG-IR-24-015)]	critical
2/28/2024	[Rockwell FactoryTalk Services Platform < 2.74 Privilege Escalation]	critical
2/28/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Cpanel-JSON-XS vulnerability (USN-6667-1)]	critical
2/28/2024	[Slackware Linux 15.0 / current wpa_supplicant Vulnerability (SSA:2024-059-01)]	critical
2/28/2024	[Debian dsa-5633 : knot-resolver - security update]	high
2/28/2024	[Oracle Linux 8 : postgresql:12 (ELSA-2024-0974)]	high
2/28/2024	[SUSE SLES15 Security Update : kernel RT (Live Patch 8 for SLE 15 SP5) (SUSE-SU-2024:0639-1)]	high
2/28/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gnutls (SUSE-SU-2024:0638-1)]	high
2/28/2024	[Fedora 38 : thunderbird (2024-5361211b10)]	high
2/28/2024	[Fedora 39 : chromium (2024-ef56ea86fc)]	high
2/28/2024	[Fedora 38 : kernel (2024-71f0f16533)]	high
2/28/2024	[Oracle Linux 9 : unbound (ELSA-2024-0977)]	high
2/28/2024	[RHEL 8 : edk2 (RHSA-2024:1013)]	high
2/28/2024	[Atlassian Confluence 6.0.1 < 7.19.18 / 7.20.x < 8.5.5 / 8.6.x < 8.7.2 / 8.8.0 (CONFSERVER-94110)]	high
2/28/2024	[RHCOS 4 : OpenShift Container Platform 4.13.35 (RHSA-2024:0948)]	high
2/28/2024	[RHEL 9 : kernel (RHSA-2024:1018)]	high
2/28/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.13.35 (RHSA-2024:0948)]	high
2/28/2024	[RHEL 9 : kernel-rt (RHSA-2024:1019)]	high
2/28/2024	[RHEL 8 : postgresql:15 (RHSA-2024:1017)]	high
2/28/2024	[Atlassian Confluence 4.0 < 7.19.19 / 7.20.x < 8.5.4 / 8.6.x < 8.6.1 / 8.7.x < 8.7.1 (CONFSERVER-94510)]	high

Datum	Schwachstelle	Bewertung
2/28/2024	[Atlassian Confluence 1.0.1 < 7.19.18 / 7.20.x < 8.5.5 / 8.6.x < 8.7.2 / 8.8.0 (CONFSERVER-94106)]	high
2/28/2024	[CBL Mariner 2.0 Security Update: moby-runc / kubevirt / kubernetes / cri-tools (CVE-2024-21626M)]	high
2/28/2024	[Ubuntu 22.04 LTS / 23.10 : Linux kernel vulnerabilities (USN-6651-2)]	high
2/28/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (AWS) vulnerabilities (USN-6653-2)]	high
2/28/2024	[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6648-2)]	high
2/28/2024	[Ubuntu 20.04 LTS / 22.04 LTS : python-openstackclient vulnerability (USN-6668-1)]	high
2/28/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Unbound vulnerabilities (USN-6665-1)]	high
2/28/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libuv vulnerability (USN-6666-1)]	high
2/28/2024	[Oracle Linux 8 : postgresql:10 (ELSA-2024-0956)]	high
2/28/2024	[Oracle Linux 8 : unbound (ELSA-2024-0965)]	high
2/28/2024	[AlmaLinux 8 : firefox (ALSA-2024:0955)]	high
2/28/2024	[AlmaLinux 8 : postgresql:13 (ALSA-2024:0975)]	high
2/28/2024	[AlmaLinux 8 : postgresql:12 (ALSA-2024:0974)]	high
2/28/2024	[AlmaLinux 8 : unbound (ALSA-2024:0965)]	high
2/28/2024	[AlmaLinux 8 : postgresql:10 (ALSA-2024:0956)]	high
2/28/2024	[AlmaLinux 9 : unbound (ALSA-2024:0977)]	high
2/28/2024	[AlmaLinux 9 : firefox (ALSA-2024:0952)]	high
2/28/2024	[AlmaLinux 9 : postgresql:15 (ALSA-2024:0950)]	high
2/28/2024	[AlmaLinux 8 : thunderbird (ALSA-2024:0964)]	high
2/28/2024	[AlmaLinux 9 : postgresql (ALSA-2024:0951)]	high
2/28/2024	[AlmaLinux 9 : thunderbird (ALSA-2024:0963)]	high

Datum	Schwachstelle	Bewertung
2/28/2024	[AlmaLinux 8 : postgresql:15 (ALSA-2024:0973)]	high
2/27/2024	[MikroTik RouterOS Insufficient Verification of Data Authenticity (CVE-2019-3979)]	high
2/27/2024	[MikroTik RouterOS Out-of-bounds Write (CVE-2021-41987)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 28 Feb 2024

Telegram For Android Connection::onReceivedData Use-After-Free

In the tgnet library used in Telegram messenger for Android, there is a use-after-free vulnerability in Connection::onReceivedData that can be triggered remotely.

- [Link](#)

—

” “Wed, 28 Feb 2024

Saflok System 6000 Key Derivation

This is a key derivation exploit for Saflokk System 6000.

- [Link](#)

—

” “Wed, 28 Feb 2024

Blood Bank 1.0 SQL Injection

Blood Bank version 1.0 suffers from multiple remote SQL injection vulnerabilities. Original discovery of SQL injection in this version is attributed to Nitin Sharma in October of 2021.

- [Link](#)

—

” “Wed, 28 Feb 2024

WordPress WP Fastest Cache 1.2.2 SQL Injection

WordPress WP Fastest Cache plugin version 1.2.2 suffers from an unauthenticated remote SQL injection vulnerability.

- [Link](#)

—

” “Wed, 28 Feb 2024

WordPress Admin Bar And Dashboard Access Control 1.28 XSS

WordPress Admin Bar and Dashboard Access Control plugin version 1.28 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

Hospital Management System 1.0 Insecure Direct Object Reference / Account Takeover

Hospital Management System version 1.0 suffers from insecure direct object reference and account takeover vulnerabilities.

- [Link](#)

—

” “Tue, 27 Feb 2024

Hospital Management System 1.0 Cross Site Scripting

Hospital Management System version 1.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

Hospital Management System 1.0 SQL Injection

Hospital Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

perl2exe 30.10C Arbitrary Code Execution

Executables created with perl2exe versions 30.10C and below suffer from an arbitrary code execution vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

Automatic-Systems SOC FL9600 FastLine Hardcoded Credentials

Automatic-Systems SOC FL9600 FastLine version V06 has hardcoded credentials for super admin functionality.

- [Link](#)

—

” “Tue, 27 Feb 2024

Automatic-Systems SOC FL9600 FastLine Directory Traversal

Automatic-Systems SOC FL9600 FastLine version V06 suffers from a directory traversal vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

Atlassian Confluence Data Center And Server Authentication Bypass

This Metasploit module exploits a broken access control vulnerability in Atlassian Confluence servers leading to an authentication bypass. A specially crafted request can be create new admin account without authentication on the target Atlassian server.

- [Link](#)

—

” “Tue, 27 Feb 2024

Moodle 4.3 Insecure Direct Object Reference

Moodle version 4.3 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

WordPress Canto Remote Shell Upload

WordPress Canto versions prior to 3.0.5 suffer from remote file inclusion and shell upload vulnerabilities.

- [Link](#)

—

” “Tue, 27 Feb 2024

WordPress Comments Like Dislike 1.2.0 Missing Authorization

WordPress Comments Like Dislike plugin versions 1.2.0 and below suffer from a missing capability check on the restore_settings function that allows an attacker to reset the plugin’s settings.

- [Link](#)

—

” “Tue, 27 Feb 2024

SuperStoreFinder 3.7 XSS / CSRF / Command Execution

SuperStoreFinder versions 3.7 and below suffer from cross site request forgery, remote command execution, and remote SQL injection vulnerabilities.

- [Link](#)

—

” “Mon, 26 Feb 2024

Simple Inventory Management System 1.0 SQL Injection

Simple Inventory Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 26 Feb 2024

Flashcard Quiz App 1.0 SQL Injection

Flashcard Quiz App version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 26 Feb 2024

FAQ Management System 1.0 SQL Injection

FAQ Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 26 Feb 2024

Backdoor.Win32.AutoSpy.10 MVID-2024-0671 Remote Command Execution

Backdoor.Win32.AutoSpy.10 malware suffers from a remote command execution vulnerability.

- [Link](#)

—

” “Sat, 24 Feb 2024

Tosibox Key Service 3.3.0 Local Privilege Escalation / Unquoted Service Path

Tosibox Key Service versions 3.3.0 and below suffer from an unquoted search path issue impacting the service Tosibox Key Service for Windows. This could potentially allow an authorized but non-privileged local user to execute arbitrary code with elevated privileges on the system.

- [Link](#)

—

” “Sat, 24 Feb 2024

Backdoor.Win32.Armageddon.r MVID-2024-0670 Hardcoded Credential

Backdoor.Win32.Armageddon.r malware suffers from a hardcoded credential vulnerability.

- [Link](#)

—

” “Sat, 24 Feb 2024

ConnectWise ScreenConnect 23.9.7 Unauthenticated Remote Code Execution

This Metasploit module exploits an authentication bypass vulnerability that allows an unauthenticated attacker to create a new administrator user account on a vulnerable ConnectWise ScreenConnect server. The attacker can leverage this to achieve remote code execution by uploading a malicious extension module. All versions of ScreenConnect version 23.9.7 and below are affected.

- [Link](#)

—

” “Sat, 24 Feb 2024

SuperCali 1.1.0 Cross Site Scripting

SuperCali version 1.1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 22 Feb 2024

QNAP QTS / QuTS Hero Unauthenticated Remote Code Execution

There exists an unauthenticated command injection vulnerability in the QNAP operating system known as QTS and QuTS hero. QTS is a core part of the firmware for numerous QNAP entry and mid-level Network Attached Storage (NAS) devices, and QuTS hero is a core part of the firmware for numerous QNAP high-end and enterprise NAS devices. The vulnerable endpoint is the quick.cgi component, exposed by the device's web based administration feature. The quick.cgi component is present in an uninitialized QNAP NAS device. This component is intended to be used during either manual or cloud based provisioning of a QNAP NAS device. Once a device has been successfully initialized, the quick.cgi component is disabled on the system. An attacker with network access to an uninitialized QNAP NAS device may perform unauthenticated command injection, allowing the attacker to execute arbitrary commands on the device.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 28 Feb 2024

ZDI-24-214: NI FlexLogger RabbitMQ Incorrect Permission Assignment Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 28 Feb 2024

ZDI-24-213: NI FlexLogger userservices Missing Authorization Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 28 Feb 2024

ZDI-24-212: NI FlexLogger TagHistorian Missing Authorization Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 28 Feb 2024

ZDI-24-211: NI FlexLogger DocumentManager Missing Authorization Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 28 Feb 2024

ZDI-24-210: NI FlexLogger SkylineService Missing Authorization Local Privilege Escalation Vul-

nerability

- [Link](#)

—

” “Wed, 28 Feb 2024

ZDI-24-209: NI FlexLogger ServiceRegistry Missing Authorization Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Mon, 26 Feb 2024

ZDI-24-208: Microsoft Azure MCR VSTS CLI vstsccli Uncontrolled Search Path Element Remote Code Execution Vulnerability

- [Link](#)

—

” “Mon, 26 Feb 2024

ZDI-24-207: Apple macOS VideoToolbox Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Mon, 26 Feb 2024

ZDI-24-206: Apple macOS ImageIO MPO Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- [Link](#)

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 EXTRABLATT: Lockbit down? UND: ScreenConnect-Lücke (10/10 kritisch)



[Zum Youtube Video](#)

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-28	Sidaction	[FRA]	Link
2024-02-27	Hôpital Sophiahemmet	[SWE]	Link
2024-02-27	Hochschule Kempten	[DEU]	Link
2024-02-25	Hamilton	[CAN]	Link
2024-02-25	Middleton-Cross Plains Area School District	[USA]	Link
2024-02-24	Thyssenkrupp (division Automobile)	[DEU]	Link
2024-02-23	Gendarmerie royale du Canada (RCMP)	[CAN]	Link
2024-02-22	Verbraucherzentrale Hessen	[DEU]	Link
2024-02-22	Coocique	[CRI]	Link
2024-02-22	City of Oakley	[USA]	Link
2024-02-22	City of Pleasant Hill	[USA]	Link
2024-02-21	Service d'immigration du Malawi	[MWI]	Link
2024-02-21	Cencora Inc	[USA]	Link
2024-02-20	Berliner Hochschule für Technik (BHT)	[DEU]	Link
2024-02-20	Continental Aerospace	[USA]	Link
2024-02-20	Change Healthcare	[USA]	Link
2024-02-19	Francis Howell School District	[USA]	Link
2024-02-19	Poughkeepsie Town	[USA]	Link
2024-02-18	Evangelische Landeskirche Hannovers	[DEU]	Link
2024-02-17	GCA (Charles André)	[FRA]	Link
2024-02-16	Government Employees Pension Fund (GEPF)	[ZAF]	Link
2024-02-15	PSI	[DEU]	Link
2024-02-15	Vili's Family Bakery	[AUS]	Link
2024-02-14	JCT600	[GBR]	Link
2024-02-14	Orange Public Schools	[USA]	Link

Datum	Opfer	Land	Information
2024-02-13	Aztech Global	[SGP]	Link
2024-02-13	Varta	[DEU]	Link
2024-02-13	Coeur d'Alene	[USA]	Link
2024-02-13	Act21	[FRA]	Link
2024-02-13	School District 67	[CAN]	Link
2024-02-12	MSH International	[CAN]	Link
2024-02-11	Centre hospitalier d'Armentières	[FRA]	Link
2024-02-11	Hipocrate Information System (HIS)	[ROU]	Link
2024-02-11	Clinique privée La Colline (groupe Hirslanden)	[CHE]	Link
2024-02-11	Consulting Radiologists Ltd.	[USA]	Link
2024-02-09	Office of Colorado State Public Defender	[USA]	Link
2024-02-09	Gouvernement des Îles Caïmans	[CYM]	Link
2024-02-07	Université de Central Missouri	[USA]	Link
2024-02-07	SouthState Bank	[USA]	Link
2024-02-07	Commune de Petersberg	[DEU]	Link
2024-02-07	Krankenhaus Lindenbrunn	[DEU]	Link
2024-02-06	Commune de Kalmar	[SWE]	Link
2024-02-06	Advania	[SWE]	Link
2024-02-06	Onclusive	[GBR]	Link
2024-02-06	Kind	[DEU]	Link
2024-02-05	Prudential Financial, Inc.	[USA]	Link
2024-02-05	Central Arkansas Library System (CALS)	[USA]	Link
2024-02-04	Northern Light Health	[USA]	Link
2024-02-04	Middletown Area School District	[USA]	Link
2024-02-02	Germantown	[USA]	Link
2024-02-02	Université de Reykjavík	[ISL]	Link

Datum	Opfer	Land	Information
2024-02-02	Hôpital de la Trinité à Lippstadt, ainsi que les cliniques associées à Erwitte et Geseke.	[DEU]	Link
2024-02-02	Mairie de Korneuburg	[AUT]	Link
2024-02-02	Welch's	[USA]	Link
2024-02-02	Etesia	[FRA]	Link
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	Link
2024-02-01	Ajuntament de Sant Antoni de Portmany	[ESP]	Link
2024-02-01	Minnesota State University-Moorhead (MSUM)	[USA]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-21	[Essential Labs]	8base	Link
2024-02-28	[Dinamic Oil]	trigona	Link
2024-02-18	[HAL Allergy]	ransomhouse	Link
2024-02-28	[Hotel Avenida, Hostal Espoz y Mina, Hostal Arriazu, Pension Alemana]	trigona	Link
2024-02-28	[easternshipbuilding.com]	lockbit3	Link
2024-02-28	[J A Piper Roofing]	blacksuit	Link
2024-02-28	[etairoshealth.com]	qilin	Link
2024-02-28	[Bangladesh Police]	mogilevich	Link
2024-02-28	[Hypertension Nephrology Associates, P.C.]	bianlian	Link
2024-02-28	[Medall Healthcare Pvt Ltd.]	bianlian	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-28	[Change Healthcare - Optum - UnitedHealth]	alphv	Link
2024-02-28	[DTN Management Company]	akira	Link
2024-02-28	[vertdure.com]	lockbit3	Link
2024-02-28	[sundbirsta.com]	lockbit3	Link
2024-02-28	[abtexelgroup.com]	cactus	Link
2024-02-28	[Frencken]	snatch	Link
2024-02-28	[Orange Public School District]	incransom	Link
2024-02-28	[Saudia MRO]	8base	Link
2024-02-28	[Bertani Trasporti Spa]	8base	Link
2024-02-28	[Acies Srl]	8base	Link
2024-02-28	[ROYAL INSIGNIA]	8base	Link
2024-02-28	[RWF Frömelt]	8base	Link
2024-02-27	[verbraucherzentrale hessen]	alphv	Link
2024-02-27	[Ireland's Department of Foreign Affairs]	mogilevich	Link
2024-02-27	[JS International]	medusa	Link
2024-02-27	[npgandour.com]	lockbit3	Link
2024-02-27	[EpicGames]	mogilevich	Link
2024-02-27	[Electro Marteix]	alphv	Link
2024-02-27	[moore-tibbits.co.uk]	threeam	Link
2024-02-27	[Ann & Robert H. Lurie Children's Hospital of Chicago]	rhapsida	Link
2024-02-27	[Hardeman County Community Health Center]	incransom	Link
2024-02-27	[WEL Partners]	incransom	Link
2024-02-26	[Ironrock]	rhapsida	Link
2024-02-26	[ch-armentieres.fr]	blackout	Link
2024-02-26	[metal7.com]	blackout	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-26	[prattindustries.com]	lockbit3	Link
2024-02-26	[PEDDIE.ORG]	clop	Link
2024-02-26	[BRADSHAW-MEDICAL.COM]	clop	Link
2024-02-26	[Penn Cinema]	medusa	Link
2024-02-16	[GCA Nederland]	ransomhouse	Link
2024-02-26	[Headwater Companies LLC]	ransomhub	Link
2024-02-26	[BAZAARVOICE.COM]	mogilevich	Link
2024-02-26	[Southwest Industrial Sales]	medusa	Link
2024-02-26	[The Professional Liability Fund]	medusa	Link
2024-02-26	[silganholdings.com]	lockbit3	Link
2024-02-26	[Angeles Medical Centers]	alphv	Link
2024-02-26	[Bjuvs kommun]	akira	Link
2024-02-26	[S+C Partners]	alphv	Link
2024-02-26	[silganholdings.com]	lockbit3	Link
2024-02-26	[ernesthealth.com]	lockbit3	Link
2024-02-14	[Abelsantosyasoc]	stormous	Link
2024-02-14	[calcomp]	stormous	Link
2024-02-15	[bombaygrills]	stormous	Link
2024-02-25	[apeagers.com.au]	lockbit3	Link
2024-02-25	[Pot O' Gold Coffee]	ciphbit	Link
2024-02-25	[AL SHEFA FARM]	ransomhub	Link
2024-02-25	[dunaway.com]	lockbit3	Link
2024-02-24	[crbgroup.com]	lockbit3	Link
2024-02-24	[nationaldentex.com]	lockbit3	Link
2024-02-24	[equilend.com]	lockbit3	Link
2024-02-24	[magierp.com]	lockbit3	Link
2024-02-24	[Spine West]	monti	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-24	[Roncelli Plastics]	bianlian	Link
2024-02-24	[Worthen Industries [FULL DATA]]	alphv	Link
2024-02-24	[GRUPOCREATIVO]	qilin	Link
2024-02-24	[kinematica.ch]	qilin	Link
2024-02-22	[Welch's]	play	Link
2024-02-23	[IJM Corporation]	hunters	Link
2024-02-23	[Family Health center]	alphv	Link
2024-02-23	[remkes.nl]	cactus	Link
2024-02-23	[APEX - apexspedition.de]	monti	Link
2024-02-23	[Acorn]	medusa	Link
2024-02-23	[Pressco Technology]	medusa	Link
2024-02-23	[ANDFLA SRL]	alphv	Link
2024-02-14	[C and J Industries, Inc.]	8base	Link
2024-02-22	[W???h?]	play	Link
2024-02-22	[team.jobs]	blackbasta	Link
2024-02-22	[Quik Pawn Shop]	akira	Link
2024-02-22	[PEER Consultants]	akira	Link
2024-02-22	[mtmrobotics.com]	threeam	Link
2024-02-22	[abcor.com.au]	threeam	Link
2024-02-22	[nflfp.com]	blackbasta	Link
2024-02-22	[climatech.com]	blackbasta	Link
2024-02-22	[usmerchants.com]	blackbasta	Link
2024-02-22	[birchallfoodservice.co.uk]	blackbasta	Link
2024-02-22	[dilweg.com]	blackbasta	Link
2024-02-22	[zircodata.com]	blackbasta	Link
2024-02-22	[Hardeman County Community Health Center]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-22	[Worthen Industries [We're giving you one last chance to save your business]]	alphv	Link
2024-02-21	[KHSS (You have 3 days)]	alphv	Link
2024-02-21	[Lancaster]	akira	Link
2024-02-21	[Desarrollo De Tecnologia y Sistemas Ltda]	akira	Link
2024-02-21	[HRTec Inc]	bianlian	Link
2024-02-21	[Marchassociates]	bianlian	Link
2024-02-21	[Austen Consultants]	alphv	Link
2024-02-21	[dasteam.ch]	blackbasta	Link
2024-02-21	[doneff.com]	threeam	Link
2024-02-21	[Helical Technology]	8base	Link
2024-02-21	[Axel Johnson]	8base	Link
2024-02-20	[INFINITIUSA.COM]	mogilevich	Link
2024-02-20	[River Delta Unified School District]	meow	Link
2024-02-20	[Finlay Screening & Crushing Systems]	hunters	Link
2024-02-20	[Raocala]	everest	Link
2024-02-20	[advancedprosolutions.com]	cactus	Link
2024-02-19	[loransrl]	qilin	Link
2024-02-19	[soco.be]	lockbit3	Link
2024-02-19	[se.com]	cactus	Link
2024-02-19	[First Professional Services]	bianlian	Link
2024-02-19	[aivi.it]	trisec	Link
2024-02-19	[ki.se]	trisec	Link
2024-02-18	[Compression Leasing Services]	dragonforce	Link
2024-02-18	[Westward 360]	dragonforce	Link
2024-02-08	[aeromechinc.com]	lockbit3	Link
2024-02-18	[carlfischer.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-17	[Bimbo Bakeries]	medusa	Link
2024-02-07	[bucher-strauss.ch]	lockbit3	Link
2024-02-16	[delia.pl]	stormous	Link
2024-02-14	[bombaygrills.com]	stormous	Link
2024-02-14	[calcomp.co.th]	stormous	Link
2024-02-02	[Abelsantosyasoc.com.ar]	stormous	Link
2024-02-18	[VSP Dental]	alphv	Link
2024-02-17	[Greater Napanee]	hunters	Link
2024-02-17	[Tiete Automobile]	hunters	Link
2024-02-17	[Voice Technologies]	hunters	Link
2024-02-17	[Afttrp]	hunters	Link
2024-02-17	[Chicago Zoological Society]	hunters	Link
2024-02-17	[BS&B Safety Systems L.L.C]	hunters	Link
2024-02-17	[Wapiti Energy]	hunters	Link
2024-02-17	[PSI]	hunters	Link
2024-02-17	[CP Communications]	hunters	Link
2024-02-16	[Prudential Financial]	alphv	Link
2024-02-16	[LoanDepot]	alphv	Link
2024-02-16	[www.cogans.ie]	trisec	Link
2024-02-16	[The Chas. E. Phipps]	medusa	Link
2024-02-16	[BRONSTEIN-CARMONA.COM]	clop	Link
2024-02-14	[davidsbridal.com]	werewolves	Link
2024-02-16	[Réseau Ribé]	hunters	Link
2024-02-16	[BRAM Auto Group]	akira	Link
2024-02-16	[etisalat.ae]	lockbit3	Link
2024-02-16	[theclosingagent.com]	lockbit3	Link
2024-02-16	[spaldingssd.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-16	[tormetal.cl]	lockbit3	Link
2024-02-16	[Concello de Teo]	hunters	Link
2024-02-16	[pacifico.co.uk]	blackbasta	Link
2024-02-16	[Ribe-Groupe]	hunters	Link
2024-02-16	[Griffin Dewatering]	hunters	Link
2024-02-15	[Dobrowski Stafford & Pierce]	bianlian	Link
2024-02-15	[LD Davis]	play	Link
2024-02-15	[von Hagen]	play	Link
2024-02-15	[Norman, Fox]	play	Link
2024-02-15	[HR Ewell & Hy-tec]	play	Link
2024-02-15	[Mechanical Reps]	play	Link
2024-02-15	[Onclusive]	play	Link
2024-02-15	[MeerServices]	play	Link
2024-02-15	[DuBose Strapping]	play	Link
2024-02-15	[SilverLining]	play	Link
2024-02-15	[Schuster Trucking Company]	hunters	Link
2024-02-15	[Asam]	akira	Link
2024-02-15	[Advantage Orthopedic & Sports Medicine Clinic]	bianlian	Link
2024-02-12	[Rush Energy Services Inc [Time's up]]	alphv	Link
2024-02-13	[Hawbaker Engineering]	snatch	Link
2024-02-15	[ASP BasilicataASM MateraIRCCS CROB]	rhysida	Link
2024-02-15	[champion.com.co]	lockbit3	Link
2024-02-15	[coreengg.com]	lockbit3	Link
2024-02-15	[sitrack.com]	lockbit3	Link
2024-02-15	[hatsinteriors.com]	lockbit3	Link
2024-02-15	[pradiergranulats.fr]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-15	[centralepaysanne.lu]	lockbit3	Link
2024-02-15	[ASA Electronics [2.7 TB]]	alphv	Link
2024-02-14	[studiogalbusera.com]	lockbit3	Link
2024-02-14	[Nekoosa School District]	akira	Link
2024-02-14	[BM Catalysts bmcatalysts.co.uk]	alphalocker	Link
2024-02-14	[vanwingerden.com]	abyss	Link
2024-02-14	[KALEEDS]	qilin	Link
2024-02-14	[conseguros]	qilin	Link
2024-02-14	[kabat.pl]	lockbit3	Link
2024-02-13	[Sindicato de Enfermería (SATSE)]	hunters	Link
2024-02-13	[wsnelson.com]	lockbit3	Link
2024-02-13	[fultoncountyga.gov]	lockbit3	Link
2024-02-14	[UNIFER]	8base	Link
2024-02-14	[Institutional Casework, Inc]	8base	Link
2024-02-14	[ATB SA Ingénieurs-conseils SIA]	8base	Link
2024-02-14	[mmiculinary.com]	lockbit3	Link
2024-02-12	[adioscancer.com]	lockbit3	Link
2024-02-14	[giraud]	qilin	Link
2024-02-13	[rajawali.com]	lockbit3	Link
2024-02-13	[motilaloswal.com]	lockbit3	Link
2024-02-13	[barberemerson.com]	blackbasta	Link
2024-02-13	[ffppkg.co.uk]	blackbasta	Link
2024-02-13	[patriziapepe.com]	blackbasta	Link
2024-02-13	[btl.info]	blackbasta	Link
2024-02-13	[globalrescue.com]	blackbasta	Link
2024-02-13	[ssmnlaw.com]	blackbasta	Link
2024-02-13	[leonardssyrups.com]	blackbasta	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-13	[ROOSENS BÉTONS]	qilin	Link
2024-02-13	[universalservicesms.com]	lockbit3	Link
2024-02-13	[Communication Federal Credit Union]	hunters	Link
2024-02-13	[doprastav.sk]	lockbit3	Link
2024-02-13	[The Source]	alphv	Link
2024-02-13	[ArcisGolf]	alphv	Link
2024-02-13	[Trans-Northern Pipelines]	alphv	Link
2024-02-13	[Herrs]	alphv	Link
2024-02-13	[Procopio]	alphv	Link
2024-02-13	[New Indy Containerboard]	alphv	Link
2024-02-13	[auruminstitute.org]	lockbit3	Link
2024-02-10	[SOPEM]	hunters	Link
2024-02-13	[Satse]	hunters	Link
2024-02-13	[Sanok Rubber CompanySpółka Akcyjna]	akira	Link
2024-02-12	[garonproducts.com]	threeam	Link
2024-02-07	[tecasrl.it]	lockbit3	Link
2024-02-12	[Antunovich Associates]	blacksuit	Link
2024-02-12	[DHX-Dependable Hawaiian Express]	knight	Link
2024-02-12	[Forgepresion.com]	cloak	Link
2024-02-12	[Rush Energy Services Inc [You have 48 hours]]	alphv	Link
2024-02-12	[SERCIDE]	alphv	Link
2024-02-12	[Lower Valley Energy, Inc]	alphv	Link
2024-02-12	[Modern Kitchens]	medusa	Link
2024-02-12	[vhprimary.com]	lockbit3	Link
2024-02-12	[germaintoiture.fr]	lockbit3	Link
2024-02-12	[Disaronno International]	meow	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-12	[Allmetal Inc.]	meow	Link
2024-02-12	[Freedom Munitions]	meow	Link
2024-02-12	[Arlington Perinatal Associates]	meow	Link
2024-02-12	[jacksonvillebeach.org]	lockbit3	Link
2024-02-12	[robs.org]	lockbit3	Link
2024-02-12	[parkhomeassist.co.uk]	lockbit3	Link
2024-02-12	[grotonschoools.org]	lockbit3	Link
2024-02-12	[isspol.gov]	lockbit3	Link
2024-02-12	[lyon.co.uk]	lockbit3	Link
2024-02-12	[dienerprecisionpumps.com]	lockbit3	Link
2024-02-12	[envie.org]	lockbit3	Link
2024-02-12	[sealco-leb.com]	lockbit3	Link
2024-02-12	[camarotto.it]	lockbit3	Link
2024-02-12	[paltertonprimary.co.uk]	lockbit3	Link
2024-02-12	[fidcornelis.be]	lockbit3	Link
2024-02-12	[plexustelerad.com]	lockbit3	Link
2024-02-12	[cabc.com.ar]	lockbit3	Link
2024-02-12	[textiles.org.tw]	lockbit3	Link
2024-02-12	[silverairways.com]	lockbit3	Link
2024-02-12	[Kreyenhop & Kluge]	hunters	Link
2024-02-12	[Kadac Australia]	medusa	Link
2024-02-11	[Amoskeag Network Consulting Group LLC]	medusa	Link
2024-02-11	[lacolline-skincare.com]	lockbit3	Link
2024-02-10	[Upper Merion Township]	qilin	Link
2024-02-10	[YKP LTDA]	ransomhub	Link
2024-02-10	[Village of Skokie]	hunters	Link
2024-02-10	[Lancaster County Sheriff's Office]	hunters	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-10	[Nastech]	hunters	Link
2024-02-10	[Benchmark Management Group]	hunters	Link
2024-02-10	[SOPEM Tunisie]	hunters	Link
2024-02-10	[Impact Energy Services]	hunters	Link
2024-02-10	[Groupe Goyette]	hunters	Link
2024-02-10	[Dalmahoy Hotel & Country Club]	hunters	Link
2024-02-10	[Carespring Health Care]	hunters	Link
2024-02-10	[Avianor Aircraft]	hunters	Link
2024-02-10	[mranet.org]	abyss	Link
2024-02-10	[aisg-online.com]	lockbit3	Link
2024-02-10	[maddockhenson]	alphv	Link
2024-02-10	[verdimed.es]	lockbit3	Link
2024-02-10	[Pacific American Fish Company Inc.]	incransom	Link
2024-02-09	[water.cc]	lockbit3	Link
2024-02-09	[CTSI]	bianlian	Link
2024-02-09	[J.P. Original]	bianlian	Link
2024-02-09	[TechNet Kronoberg AB]	bianlian	Link
2024-02-09	[Capozzi Adler, P.C.]	bianlian	Link
2024-02-09	[Drost Kivlahan McMahon & O'Connor LLC]	bianlian	Link
2024-02-09	[Grace Lutheran Foundation]	alphv	Link
2024-02-09	[ZGEO]	qilin	Link
2024-02-09	[alfiras.com]	lockbit3	Link
2024-02-09	[wannago.cloud]	qilin	Link
2024-02-09	[grupomoraval.com]	lockbit3	Link
2024-02-09	[cdtmedicus.pl]	lockbit3	Link
2024-02-09	[soken-ce.co.jp]	lockbit3	Link
2024-02-09	[maximumresearch.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-09	[indoramaventures.com]	lockbit3	Link
2024-02-09	[willislease.com]	blackbasta	Link
2024-02-09	[northseayachtsupport.nl]	lockbit3	Link
2024-02-09	[seymourct.org]	lockbit3	Link
2024-02-09	[bsaarchitects.com]	lockbit3	Link
2024-02-09	[moneyadvicetrust.org]	lockbit3	Link
2024-02-09	[posen.com]	abyss	Link
2024-02-09	[macqueeneq.com]	lockbit3	Link
2024-02-09	[parksite.com]	cactus	Link
2024-02-07	[galbusera.it]	lockbit3	Link
2024-02-08	[Ducont]	hunters	Link
2024-02-08	[perkinsmfg.com]	lockbit3	Link
2024-02-08	[originalfootwear.com]	lockbit3	Link
2024-02-08	[Jewish Home Lifecare]	alphv	Link
2024-02-08	[Distecna]	akira	Link
2024-02-07	[Western Municipal Construction]	blacksuit	Link
2024-02-07	[Southwest Binding & Laminating]	blacksuit	Link
2024-02-07	[TeraGo]	akira	Link
2024-02-07	[transaxle.com]	abyss	Link
2024-02-07	[Anderco PTE LTD]	8base	Link
2024-02-07	[Tetrosyl Group Limited]	8base	Link
2024-02-07	[Therme Laa Hotel and Silent Spa]	8base	Link
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	Link
2024-02-07	[YRW Limited - Chartered Accountants]	8base	Link
2024-02-06	[axsbolivia.com]	lockbit3	Link
2024-02-06	[vimarequipment.com]	lockbit3	Link
2024-02-06	[deltron.com]	abyss	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-06	[B&B Electric Inc]	bianlian	Link
2024-02-06	[AVer Information]	akira	Link
2024-02-06	[Celeste]	akira	Link
2024-02-06	[ArpuPlus]	medusa	Link
2024-02-06	[gocco.com]	cactus	Link
2024-02-06	[spbglobal.com]	cactus	Link
2024-02-05	[Modern Kitchens]	play	Link
2024-02-05	[Greenwich Leisure]	play	Link
2024-02-05	[Ready Mixed Concrete]	play	Link
2024-02-05	[Northeastern Sheet Metal]	play	Link
2024-02-05	[Hannon Transport]	play	Link
2024-02-05	[McMillan Pazdan Smith]	play	Link
2024-02-05	[Mason Construction]	play	Link
2024-02-05	[Albert Bartlett]	play	Link
2024-02-05	[Perry-McCall Construction]	play	Link
2024-02-05	[Virgin Islands Lottery]	play	Link
2024-02-05	[Premier Facility Management]	play	Link
2024-02-05	[Douglas County Libraries]	play	Link
2024-02-05	[Leaders Staffing]	play	Link
2024-02-06	[asecos.com]	blackbasta	Link
2024-02-05	[GRUPO SCAØRelease of all data]]	knight	Link
2024-02-05	[themisbourne.co.uk]	lockbit3	Link
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	Link
2024-02-05	[hutchpaving.com]	lockbit3	Link
2024-02-05	[davis-french-associates.co.uk]	lockbit3	Link
2024-02-05	[Campaign for Tobacco-Free Kids]	blacksuit	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-05	[VCS Observation]	akira	Link
2024-02-05	[noe.wifi.at]	lockbit3	Link
2024-02-05	[ksa-architecture.com]	lockbit3	Link
2024-02-05	[GRTC Transit System]	bianlian	Link
2024-02-05	[semesco.com]	lockbit3	Link
2024-02-05	[ultraflexx.com]	lockbit3	Link
2024-02-05	[tgestiona.br]	lockbit3	Link
2024-02-05	[philogen.com]	lockbit3	Link
2024-02-05	[prima.com]	lockbit3	Link
2024-02-05	[logtainer.com]	lockbit3	Link
2024-02-05	[portline.pt]	lockbit3	Link
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	Link
2024-02-04	[cxm.com]	lockbit3	Link
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	Link
2024-02-04	[Commonwealth Sign]	qilin	Link
2024-02-04	[FEPCO Zona Franca SAS]	knight	Link
2024-02-03	[pbwtulsa.com]	lockbit3	Link
2024-02-02	[Digitel Venezuela]	medusa	Link
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	Link
2024-02-02	[manitou-group.com]	lockbit3	Link
2024-02-02	[AbelSantosyAsociados]	knight	Link
2024-02-02	[lexcaribbean.com]	lockbit3	Link
2024-02-02	[Law Office of Michael H Joseph]	bianlian	Link
2024-02-02	[Tandem]	bianlian	Link
2024-02-02	[Innovex Downhole Solutions]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	Link
2024-02-01	[DIROX LTDA (Vietnã)]	knight	Link
2024-02-01	[etsolutions.com.mx]	threeam	Link
2024-02-01	[gatesshields.com]	lockbit3	Link
2024-02-01	[manchesterfertility.com]	lockbit3	Link
2024-02-01	[stemcor.com]	lockbit3	Link
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	Link
2024-02-01	[dms-imaging]	cuba	Link
2024-02-01	[bandcllp.com]	lockbit3	Link
2024-02-01	[taloninternational.com]	lockbit3	Link
2024-02-01	[Southwark Council]	meow	Link
2024-02-01	[Robert D. Clements Jr Law Group, LLP]	bianlian	Link
2024-02-01	[CNPC Peru S.A.]	rhysida	Link
2024-02-01	[Primeimaging database for sale]	everest	Link

8 Quellen

8.1 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>

9 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.