Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240201

Inhaltsverzeichnis

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

Linux: Sicherheitslücke in glibc bringt Angreifern Root-Privilegien

Fast alle aktuellen Linux-Varianten sind von dem Sicherheitsleck betroffen, das Missetäter jedoch nicht aus der Ferne angreifen können. Updates stehen bereit.

- Link

—

Sicherheitsupdates: DoS- und Schadcode-Attacken auf IBM ODM möglich

Angreifer können Systeme über diverse Schwachstellen in IBM Operational Decision Manager kompromittieren.

- Link

—

Google Chrome: Update schließt vier Sicherheitslücken

Google hat mit dem wöchentlichen Chrome-Update vier Sicherheitslücken geschlossen. Sie könnten das Einschleusen von Schadcode erlauben.

- Link

—

Jetzt updaten! Exploits für kritische Jenkins-Sicherheitslücke im Umlauf

Für die in der vergangenen Woche bekanntgewordene kritische Sicherheitslücke in Jenkins ist Exploit-Code aufgetaucht. Höchste Zeit zum Aktualisieren!

- Link

—

Schadcode-Attacken auf Onlineshops auf Gambio-Basis möglich

Admins von Onlineshops sollten die Gambio-Software aus Sicherheitsgründen auf den aktuellen Stand bringen.

- Link

—

Diesmal bitte patchen: Security-Update behebt kritische Schwachstelle in GitLab

GitLab 16.x enthält fünf Schwachstellen, von denen eine als kritisch eingestuft ist. Patchen ist nicht selbstverständlich, wie jüngst eine Untersuchung zeigte.

- Link

—

Microsoft Edge 121 unterstützt moderne Codecs und stopft Sicherheitslecks

Microsoft hat den Webbrowser Edge in Version 121 herausgegeben. Sie stopft eine kritische Sicherheitslücke und liefert Support für AV1-Videos.

- Link

—

Angreifer können eigene Befehle auf Juniper-Firewalls und Switches ausführen

Entwickler von Juniper haben in Junos OS mehrere Sicherheitslücken geschlossen. Noch sind aber nicht alle Updates verfügbar.

- Link

—

Automatisierungstool Jenkins: Codeschmuggel durch Sicherheitslücke möglich

Sicherheitslücken in der Open-Source-Automatisierungssoftware Jenkins erlauben Angreifern, Schadcode einzuschmuggeln. Updates helfen dem ab.

- Link

—

Cisco: Lücke erlaubt komplette Übernahme von Unified Communication-Produkten

Cisco warnt vor einer kritischen Lücke in Unified Communication-Produkten, durch die Angreifer die Kontrolle übernehmen können.

- 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	0.909010000	0.986360000	Link
CVE-2023-5360	0.967230000	0.995910000	Link
CVE-2023-4966	0.931240000	0.988830000	Link
CVE-2023-46805	0.930450000	0.988740000	Link
CVE-2023-46747	0.965530000	0.995320000	Link
CVE-2023-46604	0.971470000	0.997620000	Link
CVE-2023-42793	0.973260000	0.998690000	Link
CVE-2023-38035	0.971870000	0.997830000	Link
CVE-2023-35082	0.932740000	0.989060000	Link
CVE-2023-35078	0.955550000	0.992660000	Link
CVE-2023-34634	0.906880000	0.986120000	Link
CVE-2023-34362	0.952300000	0.991920000	Link
CVE-2023-33246	0.971270000	0.997540000	Link
CVE-2023-32315	0.963290000	0.994510000	Link
CVE-2023-30625	0.937630000	0.989580000	Link
CVE-2023-30013	0.925700000	0.988210000	Link
CVE-2023-29300	0.939750000	0.989830000	Link
CVE-2023-28771	0.923800000	0.987950000	Link
CVE-2023-27524	0.961820000	0.994070000	Link
CVE-2023-27372	0.970420000	0.997110000	Link
CVE-2023-27350	0.972430000	0.998160000	Link
CVE-2023-26469	0.927230000	0.988390000	Link
CVE-2023-26360	0.943910000	0.990480000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-26035	0.968710000	0.996480000	Link
CVE-2023-25717	0.956130000	0.992780000	Link
CVE-2023-25194	0.916080000	0.987020000	Link
CVE-2023-2479	0.958820000	0.993360000	Link
CVE-2023-24489	0.968380000	0.996330000	Link
CVE-2023-23752	0.963140000	0.994440000	Link
CVE-2023-22527	0.973010000	0.998510000	Link
CVE-2023-22518	0.965250000	0.995170000	Link
CVE-2023-22515	0.956820000	0.992930000	Link
CVE-2023-21839	0.957980000	0.993160000	Link
CVE-2023-21823	0.940060000	0.989880000	Link
CVE-2023-21554	0.961220000	0.993890000	Link
CVE-2023-20887	0.962660000	0.994260000	Link
CVE-2023-20198	0.924070000	0.988000000	Link
CVE-2023-1671	0.953130000	0.992110000	Link
CVE-2023-0669	0.968210000	0.996270000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 31 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 31 Jan 2024

[NEU] [hoch] Trustwave ModSecurity: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- Link

—

Wed, 31 Jan 2024

[NEU] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

Ein anonymer Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, einen Man-in-the-Middle-Angriff durchzuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 31 Jan 2024

[NEU] [hoch] WordPress: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann eine Schwachstelle in WordPress ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder beliebigen Code auszuführen.

- Link

—

Wed, 31 Jan 2024

[NEU] [hoch] Unify OpenScape Business: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Unify OpenScape Business ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 31 Jan 2024

[NEU] [hoch] GNU libc: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] Red Hat OpenShift Logging Subsystem: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Logging Subsystem ausnutzen, um Sicherheitsmechanismen zu umgehen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 31 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Wed, 31 Jan 2024

[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, 31 Jan 2024

[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 31 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 31 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- Link

—

Wed, 31 Jan 2024

[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen SMTP Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/1/2024	[Fedora 38 : xorg-x11-server-Xwayland (2024-05db4bcbec)]	critical
2/1/2024	[Fedora 38 : python-templated-dictionary (2024-4bd03c989b)]	critical
1/31/2024	[AlmaLinux 9 : tigervnc (ALSA-2024:0557)]	critical
1/31/2024	[AlmaLinux 8 : tigervnc (ALSA-2024:0607)]	critical
1/31/2024	[GLSA-202401-30 : X.Org X Server, XWayland: Multiple Vulnerabilities]	critical
1/31/2024	[GLSA-202401-34 : Chromium, Google Chrome, Microsoft Edge: Multiple Vulnerabilities]	critical
1/31/2024	[GLSA-202401-32 : libaom: Multiple Vulnerabilities]	critical
1/31/2024	[GLSA-202401-33 : WebKitGTK+: Multiple Vulnerabilities]	critical
1/31/2024	[RHEL 7 : tigervnc (RHSA-2024:0629)]	critical
1/31/2024	[RHEL 9 : tigervnc (RHSA-2024:0626)]	critical
1/31/2024	[RHEL 8 : tigervnc (RHSA-2024:0617)]	critical
1/31/2024	[Oracle Linux 9 : tigervnc (ELSA-2024-0557)]	critical
1/30/2024	[RHEL 8 : tigervnc (RHSA-2024:0621)]	critical
1/30/2024	[Debian dsa-5611 : glibc-doc - security update]	critical
2/1/2024	[Fedora 39 : glibc (2024-aec80d6e8a)]	high

Datum	Schwachstelle	Bewertung
2/1/2024	[Fedora 39 : thunderbird (2024-c8c2a52fb8)]	high
2/1/2024	[Fedora 38 : glibc (2024-07597a0fb3)]	high
1/31/2024	[Debian dla-3726 : bind9 - security update]	high
1/31/2024	[Fedora 38 : ncurses (2024-96090dafaf)]	high
1/31/2024	[Oracle Linux 7 : thunderbird (ELSA-2024-0601)]	high
1/31/2024	[Oracle Linux 9 : firefox (ELSA-2024-0603)]	high
1/31/2024	[GLSA-202401-31 : containerd: Multiple Vulnerabilities]	high
1/31/2024	[Debian dla-3727 : firefox-esr - security update]	high
1/31/2024	[CentOS 8 : gnutls (CESA-2024:0627)]	high
1/31/2024	[RHEL 8 : gnutls (RHSA-2024:0627)]	high
1/31/2024	[RHEL 8 : thunderbird (RHSA-2024:0619)]	high
1/31/2024	[RHEL 8 : firefox (RHSA-2024:0618)]	high
1/31/2024	[Ubuntu 20.04 LTS : runC vulnerability (USN-6619-1)]	high
1/31/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-0609)]	high
1/31/2024	[Oracle Linux 9 : thunderbird (ELSA-2024-0602)]	high
1/31/2024	[Oracle Linux 7 : firefox (ELSA-2024-0600)]	high
1/31/2024	[Oracle Linux 8 : firefox (ELSA-2024-0608)]	high
1/31/2024	[RHCOS 4 : OpenShift Container Platform 4.12.48 (RHSA-2024:0489)]	high
1/31/2024	[RHEL 8 : OpenShift Container Platform 4.12.48 (RHSA-2024:0489)]	high
1/31/2024	[Debian dla-3728 : openjdk-11-dbg - security update]	high
1/31/2024	[Cisco Nexus 9000 Information Disclosure (CVE-2023-20185)]	high
1/31/2024	[Omron CS/CJ Series (CVE-2022-45794)]	high
1/30/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Pillow vulnerabilities (USN-6618-1)]	high
1/30/2024	[Ubuntu 22.04 LTS : Linux kernel (NVIDIA) vulnerabilities (USN-6609-2)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 31 Jan 2024

XenForo 2.2.13 ArchiveImport.php Zip Slip

XenForo versions 2.2.13 and below suffer from a zip slip filename traversal vulnerability in ArchiveImport.php.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Insecure Access Control

TELSAT marKoni FM Transmitter version 1.9.5 allows an unauthorized user to change passwords.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Client-Side Access Control Bypass

TELSAT marKoni FM Transmitter version 1.9.5 implements client-side restrictions that can be bypassed by editing the HTML source page that enable administrative operations.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Backdoor Account

TELSAT marKoni FM Transmitter version 1.9.5 has a hidden super administrative account factory that has the hardcoded password inokram25 that allows full access to the web management interface configuration.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Root Command Injection

TELSAT marKoni FM Transmitter version 1.9.5 is susceptible to unauthenticated remote code execution with root privileges. An attacker can exploit a command injection vulnerability by manipulating the Email settings’ WAN IP info service, which utilizes the wget module. This allows the attacker to gain unauthorized access to the system with administrative privileges by exploiting the url parameter in the HTTP GET request to ekafcgi.fcgi.

- Link

—

” “Wed, 31 Jan 2024

glibc syslog() Heap-Based Buffer Overflow

Qualys discovered a heap-based buffer overflow in the GNU C Library's __vsyslog_internal() function, which is called by both syslog() and vsyslog(). This vulnerability was introduced in glibc 2.37 (in August 2022).

- Link

—

" "Wed, 31 Jan 2024

glibc qsort() Out-Of-Bounds Read / Write

Qualys discovered a memory corruption in the glibc's qsort() function, due to a missing bounds check. To be vulnerable, a program must call qsort() with a nontransitive comparison function (a function cmp(int a, int b) that returns (a - b), for example) and with a large number of attacker-controlled elements (to cause a malloc() failure inside qsort()). They have not tried to find such a vulnerable program in the real world. All glibc versions from at least September 1992 (glibc 1.04) to the current release (glibc 2.38) are affected, but the glibc's developers have independently discovered and patched this memory corruption in the master branch (commit b9390ba, "stdlib: Fix array bounds protection in insertion sort phase of qsort") during a recent refactoring of qsort().

- Link

—

" "Wed, 31 Jan 2024

Trojan.Win32 BankShot MVID-2024-0669 Buffer Overflow

Trojan.Win32 BankShot malware suffers from a buffer overflow vulnerability.

- Link

—

" "Wed, 31 Jan 2024

War-FTPD 1.65 Denial Of Service

War-FTPD version 1.65 remote denial of service exploit.

- Link

—

" "Wed, 31 Jan 2024

Solar FTP Server 2.1.1 Denial Of Service

Solar FTP Server version 2.1.1 remote denial of service exploit.

- Link

—

" "Wed, 31 Jan 2024

Mirth Connect 4.4.0 Remote Command Execution

A vulnerability exists within Mirth Connect due to its mishandling of deserialized data. This vulnerability can be leveraged by an attacker using a crafted HTTP request to execute OS commands within the context of the target application. The original vulnerability was identified by IHTeam and assigned

CVE-2023-37679. Later, researchers from Horizon3.ai determined the patch to be incomplete and published a gadget chain which bypassed the deny list that the original had implemented. This second vulnerability was assigned CVE-2023-43208 and was patched in Mirth Connect version 4.4.1. This Metasploit module has been tested on versions 4.1.1, 4.3.0 and 4.4.0.

- Link

—

” “Tue, 30 Jan 2024

WS_FTP Server 5.0.5 Denial Of Service

WS_FTP Server version 5.0.5 remote denial of service exploit.

- Link

—

” “Tue, 30 Jan 2024

httpdx 1.5.1 Denial Of Service

httpdx version 1.5.1 remote denial of service exploit.

- Link

—

” “Mon, 29 Jan 2024

Reprise License Manager 15.1 Privilege Escalation / File Write

Reprise License Manager version 15.1 suffers from privilege escalation and arbitrary file write vulnerabilities.

- Link

—

” “Mon, 29 Jan 2024

Jenkins 2.441 / LTS 2.426.3 Arbitrary File Read

Jenkins versions 2.441 and below and LTS 2.426.3 and below remote arbitrary file read proof of concept exploit written in Python.

- Link

—

” “Mon, 29 Jan 2024

Jenkins 2.441 / LTS 2.426.3 CVE-2024-23897 Scanner

Jenkins versions 2.441 and LTS 2.426.3 arbitrary file read scanner.

- Link

—

” “Mon, 29 Jan 2024

CSZCMS 1.3.0 SQL Injection

CSZCMS version 1.3.0 suffers from a remote SQL injection vulnerability in the admin flows.

- Link

—

” “Mon, 29 Jan 2024

PrommetriX Prometheus Metrics Leaker

PrommetriX is a tool that demonstrates a data leakage vulnerability in the Prometheus metrics-based event monitoring software.

- Link

—

” “Mon, 29 Jan 2024

Interactive Floor Plan 1.0 Cross Site Scripting

Interactive Floor Plan version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 29 Jan 2024

Chrome 121 Javascript Fork Malloc Bomb

Chrome version 121 suffers from a javascript fork malloc vulnerability that indicates memory corruption upon crash.

- Link

—

” “Mon, 29 Jan 2024

PHPJ Callback Widget 1.0 Cross Site Scripting

PHPJ Callback Widget version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 29 Jan 2024

Xitami 2.5b4 Denial Of Service

Xitami version 2.5b4 remote denial of service exploit.

- Link

—

” “Mon, 29 Jan 2024

Seattle Lab Mail 5.5 Denial Of Service

Seattle Lab Mail version 5.5 remote denial of service exploit.

- Link

—

” “Mon, 29 Jan 2024

PSOProxy 0.91 Denial Of Service

PSOProxy version 0.91 remote denial of service exploit.

- Link

—

” “Mon, 29 Jan 2024

Savant 3.0 Denial Of Service
Savant version 3.0 remote denial of service exploit.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Wed, 31 Jan 2024
ZDI-24-084: (Pwn2Own) Lexmark CX331adwe Missing Authentication Remote Code Execution Vulnerability
- Link
—
” “Wed, 31 Jan 2024
ZDI-24-083: (Pwn2Own) Lexmark CX331adwe PostScript File Parsing Memory Corruption Remote Code Execution Vulnerability
- Link
—
” “Wed, 31 Jan 2024
ZDI-24-082: (Pwn2Own) Lexmark CX331adwe PDF File Parsing Memory Corruption Remote Code Execution Vulnerability
- Link
—
” “Wed, 31 Jan 2024
ZDI-24-081: (Pwn2Own) Lexmark CX331adwe make42charstring Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Microsoft kriegt IHRE EIGENE Cloud nicht sicher konfiguriert

Zum Youtube Video

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-01-31	Caritas-Klinik Dominikus à Berlin	[DEU]	Link
2024-01-31	Viamedis	[FRA]	Link
2024-01-31	Cuba	[CUB]	Link
2024-01-29	EPS Salud Total	[COL]	Link
2024-01-28	Azienda sanitaria locale (Asp) Basilicata	[ITA]	Link
2024-01-28	Freehold Township School District	[USA]	Link
2024-01-28	Volkshochschule (Vhs) Vaterstetten	[DEU]	Link
2024-01-27	Fulton County, Georgia	[USA]	Link
2024-01-25	Group Health Cooperative of South Central Wisconsin	[USA]	Link
2024-01-25	Santa Cruz do Sul	[BRA]	Link
2024-01-24	Comté de Washington, Pennsylvanie	[USA]	Link
2024-01-24	Centre de coordination des services de communication en santé (CCSC)	[CAN]	Link
2024-01-24	The Misbourne School	[GBR]	Link
2024-01-24	Global Affairs Canada (GAC)	[CAN]	Link
2024-01-24	Linn County Sheriff’s Office	[USA]	Link
2024-01-23	Département de la Sarthe	[FRA]	Link
2024-01-23	Kansas City Area Transportation Authority (KCATA)	[USA]	Link
2024-01-23	Richmond Fellowship Scotland	[GBR]	Link
2024-01-22	EquiLend	[USA]	Link
2024-01-22	Volkshochschule (VHS) Minden-Bad Oeynhausen	[DEU]	Link
2024-01-22	ICN Business School Nancy	[FRA]	Link
2024-01-21	Bucks County	[USA]	Link
2024-01-20	Caravan and Motorhome Club (CAMC)	[GBR]	Link

Datum	Opfer	Land	Information
2024-01-19	Town of Greater Napanee	[CAN]	Link
2024-01-19	Tietoevry	[SWE]	Link
2024-01-19	Clackamas Community College	[USA]	Link
2024-01-19	Japan Food Holdings	[SGP]	Link
2024-01-17	Donau 3 FM	[DEU]	Link
2024-01-17	Service de secours de Jämtland	[SWE]	Link
2024-01-17	V.I. Lottery (Loterie des Îles Vierges)	[VIR]	Link
2024-01-17	Veolia North America	[USA]	Link
2024-01-17	Schneider Electric	[FRA]	Link
2024-01-16	Université d'État du Kansas (K-State)	[USA]	Link
2024-01-15	Foxsemicon Integrated Technology Inc (□□□□)	[TWN]	Link
2024-01-15	East Kent Services (EKS)	[GBR]	Link
2024-01-14	Douglas County Libraries	[USA]	Link
2024-01-13	Calvia	[ESP]	Link
2024-01-13	Sambr'Habitat	[BEL]	Link
2024-01-10	RE&S Holdings	[JPN]	Link
2024-01-10	Lush	[GBR]	Link
2024-01-06	loanDepot	[USA]	Link
2024-01-06	Banque nationale d'Angola	[AGO]	Link
2024-01-05	Toronto Zoo	[CAN]	Link
2024-01-05	ODAV AG	[DEU]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-31	[mnorch.org]	lockbit3	Link
2024-01-31	[apeagers.au]	lockbit3	Link
2024-01-31	[derrama.org.pe]	lockbit3	Link
2024-01-31	[Galaxy Fireworks, Inc]	medusa	Link
2024-01-31	[SportsMEDIA Technology]	alphv	Link
2024-01-31	[LeClair Group]	alphv	Link
2024-01-31	[Hydraflow]	alphv	Link
2024-01-31	[Sefin]	akira	Link
2024-01-31	[North Hill]	blacksuit	Link
2024-01-11	[Ausa]	trigona	Link
2024-01-29	[Genesis Motors]	trigona	Link
2024-01-30	[CMG Drainage Engineering]	trigona	Link
2024-01-30	[Daher Contracting]	trigona	Link
2024-01-31	[sahchicago.org]	lockbit3	Link
2024-01-31	[mrm.com.mx]	lockbit3	Link
2024-01-31	[Elliott Wave International]	8base	Link
2024-01-31	[VVD Elettrotecnica Srl]	8base	Link
2024-01-31	[Basin Trucking and Oilfield Services LLC]	8base	Link
2024-01-31	[Nbbl]	8base	Link
2024-01-31	[Meag Va-system AB]	8base	Link
2024-01-31	[Séquano]	8base	Link
2024-01-31	[Geographe]	8base	Link
2024-01-09	[Diamond Technical Services, Inc.]	8base	Link
2024-01-16	[Able One a Quadbridge Company]	8base	Link
2024-01-30	[clackamas.edu]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-30	[MA Engineering]	bianlian	Link
2024-01-30	[TECHNICA - HACKED AND MORE THEN 300 GB DATA LEAKED!]	alphv	Link
2024-01-29	[grimme.dk]	lockbit3	Link
2024-01-29	[ese.com]	lockbit3	Link
2024-01-29	[crowe.com.za]	lockbit3	Link
2024-01-25	[Lomma Crane & Rigging]	trigona	Link
2024-01-29	[Castilleja School]	akira	Link
2024-01-29	[Get Away Today]	akira	Link
2024-01-29	[Safe Plating]	akira	Link
2024-01-29	[Chamber of Deputies of Romania (Camera Deputaţilor din România)]	knight	Link
2024-01-29	[ABECOM LTDA]	knight	Link
2024-01-29	[Black Butte Coal Co]	incransom	Link
2024-01-29	[Waterford Country School Inc]	incransom	Link
2024-01-29	[Benjamin Plumbing Inc]	incransom	Link
2024-01-29	[CORBETT EXTERMINATING Inc]	incransom	Link
2024-01-29	[Dutton Brock]	alphv	Link
2024-01-29	[North American University]	incransom	Link
2024-01-28	[mordfin]	qilin	Link
2024-01-27	[oogp.com]	cactus	Link
2024-01-27	[vidalung.ai]	abyss	Link
2024-01-26	[Kansas City Area Transportation Authority]	medusa	Link
2024-01-26	[Cislo & Thomas LLP]	bianlian	Link
2024-01-26	[Image Craft]	bianlian	Link
2024-01-26	[Shoma group]	bianlian	Link
2024-01-26	[ehsd.org]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-25	[US government (private data) +Rothschild&Rockefeller]	snatch	Link
2024-01-26	[sipicorp.com]	blackbasta	Link
2024-01-26	[Brazilian Business Park]	akira	Link
2024-01-26	[elandenergy.com Eland Energy]	mydata	Link
2024-01-26	[Valley TeleCom Group]	akira	Link
2024-01-26	[securinux.net]	lockbit3	Link
2024-01-26	[jaygroup.com]	cactus	Link
2024-01-26	[Draneas Huglin Dooley LLC]	alphv	Link
2024-01-25	[Lush]	akira	Link
2024-01-25	[OrthoNY, Orthopedic Care]	incransom	Link
2024-01-25	[Four Hands LLC]	0mega	Link
2024-01-25	[CloudFire Italy]	medusa	Link
2024-01-25	[leclairgroup.com]	blackbasta	Link
2024-01-25	[NOVA Business Law Group]	bianlian	Link
2024-01-25	[The Wiser Financial Group]	bianlian	Link
2024-01-25	[ANI Networks]	akira	Link
2024-01-25	[caravanclub.co.uk]	lockbit3	Link
2024-01-25	[Toronto Zoo]	akira	Link
2024-01-25	[wannagocloud]	qilin	Link
2024-01-25	[neafidi]	qilin	Link
2024-01-24	[Brightstar Care]	alphv	Link
2024-01-24	[Hawbaker Engineering]	ransomhouse	Link
2024-01-24	[Charles Trent]	hunters	Link
2024-01-24	[Innovative Automation]	hunters	Link
2024-01-24	[Tamdown]	hunters	Link
2024-01-24	[Thorite Group]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-23	[US government (private data)]	snatch	Link
2024-01-24	[icn-artem.com]	lockbit3	Link
2024-01-24	[SANDALAWOFFICES.COM]	clop	Link
2024-01-24	[IntegrityInc.org Integrity Inc]	mydata	Link
2024-01-24	[https://www.carri.com]	mydata	Link
2024-01-24	[https://www.gadotbio.com/ Gadot Biochemical Industries Ltd]	mydata	Link
2024-01-24	[accolade-group.com + levelwear.com +Taiwan microelectronics(CRM).]	mydata	Link
2024-01-24	[a24group.com ambition24hours.co.za]	mydata	Link
2024-01-24	[https://www.mikeferry.com]	mydata	Link
2024-01-24	[Dirig Sheet Metal]	akira	Link
2024-01-24	[Winona Pattern & Mold]	meow	Link
2024-01-24	[Signature Performance Insurance]	medusa	Link
2024-01-24	[MBC Law Professional Corporation]	alphv	Link
2024-01-24	[Groupe Sweetco]	8base	Link
2024-01-24	[Bikesportz Imports]	8base	Link
2024-01-24	[La Ligue]	8base	Link
2024-01-24	[Midwest Service Center]	8base	Link
2024-01-24	[Sunfab Hydraulics AB]	8base	Link
2024-01-24	[Glimstedt]	8base	Link
2024-01-19	[FULL LEAK! Busse & Busee, PC Attorneys at Law]	alphv	Link
2024-01-23	[synergyfinancialgrp.com]	abyss	Link
2024-01-23	[micrometals.com]	abyss	Link
2024-01-23	[lyonshipyard.com]	lockbit3	Link
2024-01-23	[sierrafrontgroup.com]	lockbit3	Link
2024-01-23	[Cryopak]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-23	[fairmontfcu.com]	blackbasta	Link
2024-01-23	[ktbslaw.com]	blackbasta	Link
2024-01-23	[dupont-restauration.fr]	blackbasta	Link
2024-01-23	[kivibros.com]	blackbasta	Link
2024-01-23	[haes.ca]	blackbasta	Link
2024-01-23	[cinfab.com]	blackbasta	Link
2024-01-23	[prudentpublishing.com]	blackbasta	Link
2024-01-23	[unitedindustries.co.nz]	blackbasta	Link
2024-01-23	[stemcor.com]	blackbasta	Link
2024-01-23	[Wilhoit Properties]	akira	Link
2024-01-23	[Milestone Environmental Contracting]	akira	Link
2024-01-23	[Total Air Solutions]	alphv	Link
2024-01-22	[Double Eagle Energy Holdings IV]	hunters	Link
2024-01-23	[R.C. Moore Trucking]	hunters	Link
2024-01-23	[envea.global]	blackbasta	Link
2024-01-23	[Herrs (You have 72 hours)]	alphv	Link
2024-01-21	[Smith Capital - Press Release]	monti	Link
2024-01-16	[ARPEGE]	8base	Link
2024-01-09	[C and F Packing Company Inc.]	8base	Link
2024-01-22	[HOE Pharmaceuticals Sdn Bhd]	ransomhouse	Link
2024-01-22	[davidsbridal.com]	lockbit3	Link
2024-01-22	[agc.com]	blackbasta	Link
2024-01-22	[Double Eagle Development]	hunters	Link
2024-01-22	[southernwater.co.uk]	blackbasta	Link
2024-01-22	[Waldner’s]	medusa	Link
2024-01-22	[Pozzi Italy]	medusa	Link
2024-01-22	[The Gainsborough Bath]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-22	[Richmond Fellowship Scotland]	medusa	Link
2024-01-22	[ANS COMPUTER [72hrs]]	alphv	Link
2024-01-18	[deknudtframes.be]	cuba	Link
2024-01-21	[synnex-grp.com]	lockbit3	Link
2024-01-21	[gattoplaters.com]	lockbit3	Link
2024-01-21	[duconind.com]	lockbit3	Link
2024-01-21	[wittmann.at]	lockbit3	Link
2024-01-21	[qtc-energy.com]	lockbit3	Link
2024-01-21	[hughessupplyco.com]	lockbit3	Link
2024-01-21	[umi-tiles.com]	lockbit3	Link
2024-01-21	[cct.or.th]	lockbit3	Link
2024-01-22	[cmmt.com.tw]	lockbit3	Link
2024-01-21	[shenandoahtx.us]	lockbit3	Link
2024-01-21	[stjohnrochester.org]	lockbit3	Link
2024-01-21	[bmc-cpa.com]	lockbit3	Link
2024-01-21	[jasman.com.mx]	lockbit3	Link
2024-01-21	[North Star Tax And Accounting]	bianlian	Link
2024-01-21	[KC Pharmaceuticals]	bianlian	Link
2024-01-21	[Martinaire Aviation]	bianlian	Link
2024-01-21	[subway.com]	lockbit3	Link
2024-01-21	[tvjahnrheine.de]	lockbit3	Link
2024-01-21	[marxan.es]	lockbit3	Link
2024-01-21	[home-waremmien.be]	lockbit3	Link
2024-01-20	[wendy.mx]	lockbit3	Link
2024-01-20	[swiftair.com]	lockbit3	Link
2024-01-20	[Worthen Industries [You have three days]]	alphv	Link
2024-01-19	[Anna Jaques Hospital]	moneymessage	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-19	[pratt.edu]	lockbit3	Link
2024-01-19	[seiu1000.org]	lockbit3	Link
2024-01-19	[Sykes Consulting, Inc.]	incransom	Link
2024-01-19	[dywidag.com]	lockbit3	Link
2024-01-19	[TPG Architecture]	play	Link
2024-01-12	[jdbchina.com]	lockbit3	Link
2024-01-19	[Hamilton-Madison House]	akira	Link
2024-01-19	[Hydratek]	akira	Link
2024-01-19	[Busse & Busee, PC Attorneys at Law]	alphv	Link
2024-01-19	[evit.edu]	lockbit3	Link
2024-01-19	[Alupar Investimento SA]	hunters	Link
2024-01-19	[PROJECTSW]	qilin	Link
2024-01-19	[foxsemicon.com]	lockbit3	Link
2024-01-09	[Malongo France]	8base	Link
2024-01-18	[Samuel Sekuritas Indonesia & Samuel Aset Manajemen]	trigona	Link
2024-01-18	[Premier Facility Management]	trigona	Link
2024-01-18	[Fertility North]	trigona	Link
2024-01-18	[Vision Plast]	trigona	Link
2024-01-18	[uffs.edu.br]	stormous	Link
2024-01-18	[Groveport Madison Schools]	blacksuit	Link
2024-01-18	[GROWTH by NCRC]	bianlian	Link
2024-01-18	[LT Business Dynamics]	bianlian	Link
2024-01-18	[digipwr.com]	lockbit3	Link
2024-01-18	[jaffeandasher.com]	lockbit3	Link
2024-01-18	[Gallup McKinley County Schools]	hunters	Link
2024-01-15	[aercap.com]	slug	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-17	[DENHAM the Jeanmaker]	akira	Link
2024-01-17	[Stone, Avant & Daniels]	medusa	Link
2024-01-17	[JspPharma]	insane	Link
2024-01-16	[Axfast AB]	8base	Link
2024-01-16	[Syndicat Général des Vignerons de la Champagne]	8base	Link
2024-01-16	[Washtech]	8base	Link
2024-01-16	[SIVAM Coatings S.p.A.]	8base	Link
2024-01-16	[Nexus Telecom Switzerland AG]	8base	Link
2024-01-16	[millgate.co.uk]	lockbit3	Link
2024-01-16	[Becker Logistics]	akira	Link
2024-01-16	[Bestway Sales]	akira	Link
2024-01-16	[TGS Transportation]	akira	Link
2024-01-16	[Premium Guard]	akira	Link
2024-01-16	[F J O’Hara & Sons]	qilin	Link
2024-01-16	[Donear Industries]	bianlian	Link
2024-01-15	[Beit Handesai]	malekteam	Link
2024-01-15	[shinwajpn.co.jp]	lockbit3	Link
2024-01-15	[maisonsdelavenir.com]	lockbit3	Link
2024-01-15	[vasudhapharma.com]	lockbit3	Link
2024-01-15	[hosted-it.co.uk]	lockbit3	Link
2024-01-15	[Ausa]	hunters	Link
2024-01-15	[Republic Shipping Consolidators, Inc]	bianlian	Link
2024-01-15	[Northeast Spine and Sports Medicine’s]	bianlian	Link
2024-01-14	[SPARTAN Light Metal Products]	unsafe	Link
2024-01-14	[Hartl European Transport Company]	unsafe	Link
2024-01-14	[American International College]	unsafe	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-14	[www.kai.id “FF”]	stormous	Link
2024-01-14	[amenitek.com]	lockbit3	Link
2024-01-08	[turascandinavia.com]	lockbit3	Link
2024-01-13	[Lee Spring]	rhysida	Link
2024-01-11	[Charm Sciences]	snatch	Link
2024-01-11	[Malabar Gold & Diamonds]	snatch	Link
2024-01-11	[Banco Promerica]	snatch	Link
2024-01-12	[arrowinternational.com]	lockbit3	Link
2024-01-12	[thecsi.com]	threeam	Link
2024-01-12	[pharrusa.com]	threeam	Link
2024-01-12	[Builcore]	alphv	Link
2024-01-12	[hotelcontinental.no]	qilin	Link
2024-01-12	[olea.com]	lockbit3	Link
2024-01-12	[asburyauto.com]	cactus	Link
2024-01-12	[Washington School For The Deaf]	incransom	Link
2024-01-12	[Former S.p.A.]	8base	Link
2024-01-12	[International Trade Brokers and Forwarders]	8base	Link
2024-01-12	[BALLAY MENUISERIES]	8base	Link
2024-01-12	[Anderson King Energy Consultants, LLC]	8base	Link
2024-01-12	[Sems and Specials Incorporated]	8base	Link
2024-01-12	[acutis.com]	cactus	Link
2024-01-12	[dtsolutions.net]	cactus	Link
2024-01-12	[intercityinvestments.com]	cactus	Link
2024-01-12	[hi-cone.com]	cactus	Link
2024-01-12	[Alliedwoundcare]	everest	Link
2024-01-12	[Primeimaging]	everest	Link
2024-01-11	[Blackburn College]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-11	[Vincentz Network]	akira	Link
2024-01-11	[Limburg]	medusa	Link
2024-01-11	[Water For People]	medusa	Link
2024-01-11	[pactchangeslives.com]	lockbit3	Link
2024-01-11	[Triella]	alphv	Link
2024-01-11	[Ursel Phillips Fellows Hopkinson]	alphv	Link
2024-01-11	[SHIBLEY RIGHTON]	alphv	Link
2024-01-11	[automotionshade.com]	alphv	Link
2024-01-11	[R Robertson Insurance Brokers]	alphv	Link
2024-01-10	[molnar&partner]	qilin	Link
2024-01-10	[hartalega.com.my]	lockbit3	Link
2024-01-10	[agnesb.eu]	lockbit3	Link
2024-01-10	[twt.co.za]	lockbit3	Link
2024-01-10	[tiautoinvestments.co.za]	lockbit3	Link
2024-01-10	[Group Bogart]	alphv	Link
2024-01-09	[Delco Automation]	blacksuit	Link
2024-01-09	[Viridi]	akira	Link
2024-01-09	[Ito Pallpack Gruppen]	akira	Link
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	Link
2024-01-09	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	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.