Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240920

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

Kritische SAML-Anmelde-Lücke mit Höchstwertung gefährdet Gitlab-Server

Unter bestimmten Voraussetzungen können sich Angreifer Zugriff auf die DevSecOps-Plattform Gitlab verschaffen.

- Link

—

Sicherheitsupdates: BIOS-Lücken gefährden Dell-Computer

Unter anderem sind bestimmte Computer von Dells Alienware-Serie attackierbar. Sicherheitspatches stehen zum Download.

- Link

—

Sicherheitslücken: Netzwerk-Controller und -Gateways von Aruba sind verwundbar

Angreifer können Netzwerkgeräte von HPE Aruba attackieren und im schlimmsten Fall Appliances kompromittieren.

- Link

—

VMware vCenter: Angreifer aus dem Netz können Schadcode einschleusen

Broadcom stopft mehrere Sicherheitslücken in VMware vCenter. Schlimmstenfalls können Angreifer aus dem Netz Schadcode einschmuggeln und ausführen.

- Link

—

Samsung-Druckertreiber ermöglichen Angreifern Rechteausweitung

Für Samsungs Office-Drucker stellt HP einen aktualisierten Universal-Treiber für Windows bereit. Er dichtet ein Rechteausweitungsleck ab.

- Link

—

Angreifer attackieren Sicherheitslücken in Microsofts MSHTML und Whatsup Gold

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt vor Angriffen auf Sicherheitslücken in Microsofts MSHTML und Whatsup Gold.

- Link

—

Sicherheitspatch: Hintertür in einigen D-Link-Routern erlaubt unbefugte Zugriffe

Angreifer können bestimmte Router-Modelle von D-Link attackieren und kompromittieren. Sicherheitsupdates stehen zum Download bereit.

- Link

—

Sicherheitspatch verfügbar: Angriffe auf Ivanti Cloud Service Appliance

Derzeit attackieren Angreifer Ivanti Cloud Service Appliances mit Schadcode. Außedem könnten Attacken auf Endpoint Manager bevorstehen.

- Link

—

Lenovo schließt Lücken in BIOS, Management-Controller und WLAN-Treiber

Wichtige Sicherheitsupdates schützen Computer von Lenovo. Im schlimmsten Fall können Angreifer Schadcode ausführen.

- Link

—

Solarwinds ARM: Unbefugte Zugriffe und Schadcode-Attacken möglich

Die Solarwinds-Entwickler haben zwei Sicherheitslücken in Access Rights Manager geschlossen. Eine Lücke gilt als kritisch.

- 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-2023-7028	0.957050000	0.994730000	Link
CVE-2023-6895	0.927330000	0.990670000	Link
CVE-2023-6553	0.947820000	0.993100000	Link
CVE-2023-6019	0.918710000	0.989860000	Link
CVE-2023-52251	0.945480000	0.992740000	Link
CVE-2023-4966	0.970840000	0.998140000	Link
CVE-2023-49103	0.949680000	0.993410000	Link
CVE-2023-48795	0.965330000	0.996450000	Link
CVE-2023-47246	0.961220000	0.995430000	Link
CVE-2023-46805	0.950230000	0.993500000	Link
CVE-2023-46747	0.971020000	0.998230000	Link
CVE-2023-46604	0.969070000	0.997510000	Link
CVE-2023-4542	0.948590000	0.993220000	Link
CVE-2023-43208	0.973740000	0.999270000	Link
CVE-2023-43177	0.961480000	0.995490000	Link
CVE-2023-42793	0.972380000	0.998700000	Link
CVE-2023-41265	0.907590000	0.989110000	Link
CVE-2023-39143	0.940700000	0.992190000	Link
CVE-2023-38205	0.950330000	0.993510000	Link
CVE-2023-38203	0.965830000	0.996580000	Link
CVE-2023-38146	0.919150000	0.989900000	Link
CVE-2023-38035	0.974690000	0.999710000	Link
CVE-2023-36845	0.967850000	0.997130000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965910000	0.996600000	Link
CVE-2023-35082	0.966710000	0.996810000	Link
CVE-2023-35078	0.970930000	0.998180000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34960	0.900520000	0.988670000	Link
CVE-2023-34634	0.923140000	0.990270000	Link
CVE-2023-34362	0.970450000	0.997980000	Link
CVE-2023-34039	0.945100000	0.992680000	Link
CVE-2023-3368	0.939780000	0.992070000	Link
CVE-2023-33246	0.967830000	0.997130000	Link
CVE-2023-32315	0.971490000	0.998380000	Link
CVE-2023-30625	0.953610000	0.994120000	Link
CVE-2023-30013	0.965950000	0.996610000	Link
CVE-2023-29300	0.969240000	0.997550000	Link
CVE-2023-29298	0.970810000	0.998110000	Link
CVE-2023-28432	0.920500000	0.990040000	Link
CVE-2023-28343	0.933130000	0.991340000	Link
CVE-2023-28121	0.925430000	0.990500000	Link
CVE-2023-27524	0.970600000	0.998010000	Link
CVE-2023-27372	0.973930000	0.999360000	Link
CVE-2023-27350	0.969520000	0.997630000	Link
CVE-2023-26469	0.953540000	0.994090000	Link
CVE-2023-26360	0.964390000	0.996140000	Link
CVE-2023-26035	0.968720000	0.997390000	Link
CVE-2023-25717	0.954660000	0.994290000	Link
CVE-2023-25194	0.965150000	0.996370000	Link
CVE-2023-2479	0.963230000	0.995840000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.973150000	0.999040000	Link
CVE-2023-23752	0.951460000	0.993680000	Link
CVE-2023-23333	0.960430000	0.995250000	Link
CVE-2023-22527	0.970940000	0.998190000	Link
CVE-2023-22518	0.957870000	0.994840000	Link
CVE-2023-22515	0.973160000	0.999060000	Link
CVE-2023-21839	0.951270000	0.993640000	Link
CVE-2023-21554	0.955880000	0.994510000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962220000	0.995630000	Link
CVE-2023-0669	0.971300000	0.998340000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 19 Sep 2024

[UPDATE] [hoch] Wireshark: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Wireshark ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Thu, 19 Sep 2024

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

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen

Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 19 Sep 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [kritisch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Verfügbarkeit, Vertraulichkeit und Integrität zu gefährden.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, einen Denial of Service Zustand auszulösen und mehrere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [kritisch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Daten zu manipulieren und seine Privilegien zu erweitern.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder

Code auszuführen.
- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.
- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.
- Link

—

Thu, 19 Sep 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.
- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.
- Link

—

Thu, 19 Sep 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.
- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 19 Sep 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- Link

—

Thu, 19 Sep 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 19 Sep 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Thu, 19 Sep 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder Daten zu manipulieren.

- Link

—

Thu, 19 Sep 2024

[NEU] [hoch] CoreDNS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CoreDNS ausnutzen, um einen

Denial of Service Angriff durchzuführen oder ein DNS-Cache-Poisoning durchzuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/19/2024	[Oracle Linux 9 : thunderbird (ELSA-2024-6683)]	critical
9/19/2024	[Oracle Linux 9 : firefox (ELSA-2024-6681)]	critical
9/19/2024	[Oracle Linux 9 : expat (ELSA-2024-6754)]	critical
9/19/2024	[Oracle Linux 8 : firefox (ELSA-2024-6682)]	critical
9/19/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-6684)]	critical
9/19/2024	[FreeBSD : Gitlab – vulnerabilities (3e738678-7582-11ef-bece-2cf05da270f3)]	critical
9/19/2024	[RHEL 8 : thunderbird (RHSA-2024:6816)]	critical
9/19/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Git vulnerabilities (USN-7023-1)]	critical
9/19/2024	[Docker Desktop < 4.34.2 Multiple Vulnerabilities]	critical
9/19/2024	[Docker Desktop < 4.34.2 Multiple Vulnerabilities]	critical
9/19/2024	[Docker Desktop < 4.34.2 Multiple Vulnerabilities]	critical
9/19/2024	[RHEL 7 : firefox update (Important) (RHSA-2024:6838)]	critical
9/19/2024	[Ubuntu 20.04 LTS : tgt vulnerability (USN-7024-1)]	critical
9/19/2024	[VMware vCenter Server 7.x < 7.0 U3s / 8.x < 8.0 U3b Multiple Vulnerabilities (VMSA-2024-0019)]	critical
9/19/2024	[RHEL 8 : firefox update (Important) (RHSA-2024:6891)]	critical
9/19/2024	[RHEL 8 : firefox update (Important) (RHSA-2024:6892)]	critical
9/19/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Emacs vulnerabilities (USN-7027-1)]	critical

Datum	Schwachstelle	Bewertung
9/19/2024	[RHEL 9 : openssl (RHSA-2024:6783)]	high
9/19/2024	[Oracle Linux 9 : qemu-kvm (ELSA-2024-12674)]	high
9/19/2024	[RHEL 8 : edk2 (RHSA-2024:6845)]	high
9/19/2024	[CBL Mariner 2.0 Security Update: curl (CVE-2024-6197_-_A)]	high
9/19/2024	[Ubuntu 20.04 LTS / 22.04 LTS : LibreOffice vulnerability (USN-7025-1)]	high
9/19/2024	[RHEL 8 : edk2 (RHSA-2024:6849)]	high
9/19/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-7015-2)]	high
9/19/2024	[LibreOffice 24.2.x < 24.2.5 / 24.8.0 (CVE-2024-7788)]	high
9/19/2024	[Debian dsa-5773 : chromium - security update]	high
9/19/2024	[Oracle Linux 9 : openssl (ELSA-2024-6783)]	high
9/19/2024	[Oracle Linux 8 : ruby:3.3 (ELSA-2024-6784)]	high
9/19/2024	[Oracle Linux 9 : ruby:3.3 (ELSA-2024-6785)]	high
9/19/2024	[RHEL 9 : Red Hat Single Sign-On 7.6.11 security update on RHEL 9 (Important) (RHSA-2024:6880)]	high
9/19/2024	[RHEL 7 : Red Hat Single Sign-On 7.6.11 security update on RHEL 7 (Important) (RHSA-2024:6878)]	high
9/19/2024	[RHEL 8 : Red Hat Single Sign-On 7.6.11 security update on RHEL 8 (Important) (RHSA-2024:6879)]	high
9/19/2024	[Ubuntu 16.04 LTS : PostgreSQL vulnerability (USN-6968-2)]	high
9/19/2024	[EulerOS 2.0 SP12 : openssh (EulerOS-SA-2024-2454)]	high
9/19/2024	[EulerOS 2.0 SP12 : openssh (EulerOS-SA-2024-2455)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 19 Sep 2024

htmly 2.9.9 Cross Site Scripting

htmly version 2.9.9 suffers from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Thu, 19 Sep 2024

WordPress LMS 4.2.7 SQL Injection

WordPress LMS plugin versions 4.2.7 and below suffer from a remote SQL injection vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Nexus Repository Manager 3 Path Traversal

Proof of concept exploit that demonstrates an unauthenticated path traversal vulnerability in Nexus Repository Manager version 3.

- Link

—

” “Thu, 19 Sep 2024

Check Point Security Gateways Information Disclosure

Proof of concept exploit that demonstrates an information disclosure vulnerability in Check Point Security Gateways.

- Link

—

” “Thu, 19 Sep 2024

Telerik Report Server 2024 Q1 Authentication Bypass

In Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier, on IIS, an unauthenticated attacker can gain access to Telerik Report Server restricted functionality via an authentication bypass vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Prison Management System 1.0 Code Injection

Prison Management System version 1.0 suffers from a PHP code injection vulnerability.

- Link

—

” “Thu, 19 Sep 2024

PreSchool Enrollment System 1.0 SQL Injection

PreSchool Enrollment System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 19 Sep 2024

SchoolPlus 1.0 Cross Site Request Forgery

SchoolPlus version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Online Security Guard Hiring System 1.0 Insecure Settings

Online Security Guard Hiring System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Online Food Management System 1.0 SQL Injection

Online Food Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 19 Sep 2024

SPIP BigUp 4.1.17 Code Injection

SPIP BigUp version 4.1.17 suffers from a remote PHP code injection vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Online Exam System 1.0 Information Disclosure

Online Exam System version 1.0 suffers from an information disclosure vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Old Age Home Management System 1.0 Insecure Settings

Old Age Home Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Nipah Virus Testing Management System 1.0 Insecure Settings

Nipah Virus Testing Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Thu, 19 Sep 2024

Men Salon Management System 2.0 Insecure Settings

Men Salon Management System version 2.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 18 Sep 2024

Online Traffic Offense 1.0 CSRF / Arbitrary File Upload

Online Traffic Offense version 1.0 suffers from cross site request forgery and arbitrary file upload vulnerabilities.

- Link

—

” “Wed, 18 Sep 2024

Backdoor.Win32.CCInvader.10 MVID-2024-0694 Authentication Bypass

Backdoor.Win32.CCInvader.10 malware suffers from a bypass vulnerability.

- Link

—

” “Wed, 18 Sep 2024

Backdoor.Win32.BlackAngel.13 MVID-2024-0695 Code Execution

Backdoor.Win32.BlackAngel.13 malware suffers from a code execution vulnerability.

- Link

—

” “Wed, 18 Sep 2024

Backdoor.Win32.Delf.yj MVID-2024-0693 Information Disclosure

Backdoor.Win32.Delf.yj malware suffers from an information leakage vulnerability.

- Link

—

” “Wed, 18 Sep 2024

Online Exam System 1.0 Insecure Settings

Online Exam System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 18 Sep 2024

Online Bus Ticket Booking Website 1.0 SQL Injection

Online Bus Ticket Booking Website version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 18 Sep 2024

Nipah Virus Testing Management System 1.0 SQL Injection

Nipah Virus Testing Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 18 Sep 2024

Membership Management System 1.1 SQL Injection

Membership Management System version 1.1 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 18 Sep 2024

HYSCALE System 1.9 Add Administrator / Cross Site Request Forgery

HYSCALE System version 1.9 suffers from add administrator and cross site request forgery vulnerabilities.

- Link

—

” “Wed, 18 Sep 2024

Furniture Master 2 SQL Injection

Furniture Master version 2 suffers from a remote SQL injection vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 17 Sep 2024

ZDI-24-1272: PDF-XChange Editor AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1271: PDF-XChange Editor AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1270: PDF-XChange Editor Doc Object Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1269: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1268: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1267: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1266: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1265: PDF-XChange Editor RTF File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1264: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1263: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1262: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1261: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1260: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1259: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1258: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1257: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1256: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1255: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1254: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1253: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1252: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1251: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1250: PDF-XChange Editor PPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1249: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1248: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1247: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1246: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1245: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1244: PDF-XChange Editor U3D File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1243: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1242: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1241: PDF-XChange Editor U3D File Parsing Use-After-Free Remote Code Execution Vul-

nerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1240: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1239: PDF-XChange Editor U3D File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1238: PDF-XChange Editor U3D File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1237: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1236: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1235: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1234: WinZip Mark-of-the-Web Bypass Vulnerability

- Link

—

” “Tue, 17 Sep 2024

ZDI-24-1233: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability
- Link

—

” “Tue, 17 Sep 2024
ZDI-24-1232: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability
- Link

—

” “Tue, 17 Sep 2024
ZDI-24-1231: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability
- Link

—

” “Tue, 17 Sep 2024
ZDI-24-1230: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability
- Link

—

” “Tue, 17 Sep 2024
ZDI-24-1229: BlueZ HID over GATT Profile Improper Access Control Remote Code Execution Vulnerability
- Link

—

” “Tue, 17 Sep 2024
ZDI-24-1228: Trend Micro Deep Discovery Inspector SQL Injection Information Disclosure Vulnerability
- Link

—

” “Tue, 17 Sep 2024
ZDI-24-1227: Trend Micro Deep Discovery Inspector SQL Injection Information Disclosure Vulnerability
- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection.

Zum Youtube Video

6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-16	TAAG	[AGO]	Link
2024-09-16	Heinrich-Böll-Gesamtschule et Rurtal-Gymnasium	[DEU]	Link
2024-09-16	Fylde Coast Academy Trust	[GBR]	Link
2024-09-15	Radio Geretsried	[DEU]	Link
2024-09-14	Zacros	[JPN]	Link
2024-09-12	⊠⊠⊠⊠⊠⊠ (Kantsu)	[JPN]	Link
2024-09-12	LolaLiza	[BEL]	Link
2024-09-11	Providence Public School District (PPSD)	[USA]	Link
2024-09-09	Université de Gênes	[ITA]	Link
2024-09-08	Highline Public Schools	[USA]	Link
2024-09-08	Groupe Bayard	[FRA]	Link
2024-09-08	Isbergues	[FRA]	Link
2024-09-06	Superior Tribunal de Justiça (STJ)	[BRA]	Link
2024-09-05	Air-e	[COL]	Link
2024-09-05	Charles Darwin School	[GBR]	Link
2024-09-05	Elektroskandia	[SWE]	Link
2024-09-04	Tewkesbury Borough Council	[GBR]	Link
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	Link
2024-09-04	Compass Group	[AUS]	Link
2024-09-02	Transport for London (TfL)	[GBR]	Link
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	Link
2024-09-02	Kawasaki Motors Europe	[GBR]	Link
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-19	[rarholding.com]	ransomhub	Link
2024-09-19	[Fritzøe Engros]	medusa	Link
2024-09-19	[Wilson & Lafleur]	medusa	Link
2024-09-19	[Wertachkliniken.de]	cloak	Link
2024-09-19	[newriverelectrical.com]	ElDorado	Link
2024-09-19	[seaglesafety.com]	ElDorado	Link
2024-09-19	[rccauto.com]	ElDorado	Link
2024-09-19	[itasnatta.edu.it]	ElDorado	Link
2024-09-19	[a1mobilelock.com]	ElDorado	Link
2024-09-19	[curvc.com]	ElDorado	Link
2024-09-19	[patricksanderscompany.com]	ElDorado	Link
2024-09-19	[thinksimple.com]	ElDorado	Link
2024-09-19	[pesprograms.com]	ElDorado	Link
2024-09-19	[palmfs.com]	ElDorado	Link
2024-09-19	[kennedyfunding.com]	ElDorado	Link
2024-09-19	[advbe.com]	ransomhub	Link
2024-09-19	[Sunrise Farms]	fog	Link
2024-09-19	[Nusser Mineralöl GmbH]	incransom	Link
2024-09-19	[avl1.com]	ransomhub	Link
2024-09-19	[libertyfirstcu.com]	ransomhub	Link
2024-09-19	[Hunter Dickinson Inc.]	bianlian	Link
2024-09-19	[tims.com]	abyss	Link
2024-09-18	[bspcr.com]	lockbit3	Link
2024-09-18	[lakelandchamber.com]	lockbit3	Link
2024-09-18	[yesmoke.eu]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-18	[efile.com]	lockbit3	Link
2024-09-18	[paybito.com]	lockbit3	Link
2024-09-18	[Compass Group (2nd attack)]	medusa	Link
2024-09-18	[Structural Concepts]	medusa	Link
2024-09-19	[Vidisco]	handala	Link
2024-09-19	[IIB (Israeli Industrial Batteries)]	handala	Link
2024-09-18	[Plaisted Companies]	play	Link
2024-09-11	[Bertelkamp Automation]	qilin	Link
2024-09-18	[DJH Jugendherberge]	hunters	Link
2024-09-18	[Prentke Romich Company]	fog	Link
2024-09-12	[agricola]	qilin	Link
2024-09-16	[Amerinational Community Services]	medusa	Link
2024-09-16	[Providence Public School Department]	medusa	Link
2024-09-16	[AZPIRED]	medusa	Link
2024-09-17	[Compass Group]	medusa	Link
2024-09-18	[Chernan Technology]	orca	Link
2024-09-18	[Port of Seattle/Seattle-Tacoma International Airport (SEA)]	rhysida	Link
2024-09-16	[Baskervill]	play	Link
2024-09-16	[Protective Industrial Products]	play	Link
2024-09-16	[Inktel]	play	Link
2024-09-16	[Rsp]	play	Link
2024-09-16	[Hariri Pontarini Architects]	play	Link
2024-09-16	[Multidata]	play	Link
2024-09-18	[Environmental Code Consultants Inc]	meow	Link
2024-09-18	[EnviroNET Inc]	meow	Link
2024-09-18	[Robson Planning Group Inc]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-16	[oipip.gda.pl]	ransomhub	Link
2024-09-16	[kryptonresources.com]	ransomhub	Link
2024-09-16	[www.tta.cls]	ransomhub	Link
2024-09-18	[globe.com.bd]	ValenciaLeaks	Link
2024-09-18	[satiagroup.com]	ValenciaLeaks	Link
2024-09-18	[duopharmabiotech.com]	ValenciaLeaks	Link
2024-09-18	[tendam.es]	ValenciaLeaks	Link
2024-09-18	[cityofpleasantonca.gov]	ValenciaLeaks	Link
2024-09-16	[www.faithfc.org]	ransomhub	Link
2024-09-16	[www.adantia.es]	ransomhub	Link
2024-09-16	[topdoctors.com]	ransomhub	Link
2024-09-16	[www.8010urbanliving.com]	ransomhub	Link
2024-09-16	[www.taperuvicha.com]	ransomhub	Link
2024-09-17	[www.plumbersstock.com]	ransomhub	Link
2024-09-17	[www.nikpol.com.au]	ransomhub	Link
2024-09-18	[www.galloway-macleod.co.uk]	ransomhub	Link
2024-09-18	[ringpower.com]	ransomhub	Link
2024-09-17	[miit.gov.cn]	killsec	Link
2024-09-17	[New Electric]	hunters	Link
2024-09-17	[AutoCanada]	hunters	Link
2024-09-17	[natcoglobal.com]	cactus	Link
2024-09-17	[Sherr Puttmann Akins Lamb PC]	bianlian	Link
2024-09-17	[peerlessumbrella.com]	cactus	Link
2024-09-17	[thomas-lloyd.com]	cactus	Link
2024-09-16	[Cruz Marine (cruz.local)]	lynx	Link
2024-09-16	[SuperCommerce.ai]	killsec	Link
2024-09-16	[MCNA Dental 1 million patients records]	everest	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-16	[ExcelPlast Tunisie]	orca	Link
2024-09-16	[northernsafety.com]	blackbasta	Link
2024-09-16	[thompsoncreek.com]	blackbasta	Link
2024-09-07	[www.atlcc.net]	ransomhub	Link
2024-09-10	[accuraterailroad.com]	ransomhub	Link
2024-09-10	[advantagecdc.org]	ransomhub	Link
2024-09-10	[lafuturasrl.it]	ransomhub	Link
2024-09-15	[dowley.com]	lockbit3	Link
2024-09-15	[apexbrasil.com.br]	lockbit3	Link
2024-09-15	[fivestarproducts.com]	lockbit3	Link
2024-09-15	[ignitarium.com]	lockbit3	Link
2024-09-15	[nfcaa.org]	lockbit3	Link
2024-09-15	[Emtel]	arcusmedia	Link
2024-09-15	[EAGLE School]	qilin	Link
2024-09-15	[salaam.af]	lockbit3	Link
2024-09-15	[INTERNAL.ROCKYMOUNTAINGASTRO.COM]	trinity	Link
2024-09-14	[Gino Giglio Generation Spa]	arcusmedia	Link
2024-09-14	[Rextech]	arcusmedia	Link
2024-09-14	[Like Family's]	arcusmedia	Link
2024-09-14	[UNI-PA A.Ş]	arcusmedia	Link
2024-09-12	[OnePoint Patient Care]	incransom	Link
2024-09-14	[Retemex]	ransomexx	Link
2024-09-14	[ORCHID-ORTHO.COM]	clop	Link
2024-09-11	[jatelindo]	stormous	Link
2024-09-13	[mivideo.club]	stormous	Link
2024-09-12	[Micron Internet]	medusa	Link
2024-09-12	[TECHNOLOG S.r.l.]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-14	[ecbawm.com]	abyss	Link
2024-09-13	[FD Lawrence Electric]	blacksuit	Link
2024-09-13	[True Family Enterprises]	play	Link
2024-09-13	[Dimensional Merchandising]	play	Link
2024-09-13	[Creative Playthings]	play	Link
2024-09-13	[Law Offices of Michael J Gurfinkel, Inc]	bianlian	Link
2024-09-13	[Hostetler Buildings]	blacksuit	Link
2024-09-13	[VIcom Corporation]	hunters	Link
2024-09-13	[Arch-Con]	hunters	Link
2024-09-13	[HB Construction]	hunters	Link
2024-09-13	[Associated Building Specialties]	hunters	Link
2024-09-12	[www.southeasternretina.com]	ransomhub	Link
2024-09-11	[Ascend Analytics (ascendanalytics.com)]	lynx	Link
2024-09-06	[Kingsmill Resort]	qilin	Link
2024-09-12	[brunswickhospitalcenter.org]	threeam	Link
2024-09-12	[Carpenter McCadden and Lane LLP]	meow	Link
2024-09-12	[CSMR Agrupación de Colaboración Empresaria]	meow	Link
2024-09-11	[ICBC (London)]	hunters	Link
2024-09-12	[thornton-inc.com]	ransomhub	Link
2024-09-04	[nhbg.com.co]	lockbit3	Link
2024-09-12	[mechdyne.com]	ransomhub	Link
2024-09-10	[Starr-Iva Water & Sewer District]	medusa	Link
2024-09-10	[Karakaya Group]	medusa	Link
2024-09-10	[allamericanpoly.com]	ransomhub	Link
2024-09-11	[Charles Darwin School]	blacksuit	Link
2024-09-11	[S. Walter Packaging]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-11	[Clatronic International GmbH]	fog	Link
2024-09-11	[Advanced Physician Management Services LLC]	meow	Link
2024-09-11	[Arville]	meow	Link
2024-09-11	[ICBC London]	hunters	Link
2024-09-11	[Ladov Law Firm]	bianlian	Link
2024-09-10	[Regent Care Center]	incransom	Link
2024-09-10	[www.vinatiorganics.com]	ransomhub	Link
2024-09-10	[Evans Distribution Systems]	play	Link
2024-09-10	[Weldco-Beales Manufacturing]	play	Link
2024-09-10	[PIGGLY WIGGLY ALABAMA DISTRIBUTING]	play	Link
2024-09-10	[Elgin Separation Solutions]	play	Link
2024-09-10	[Bel-Air Bay Club]	play	Link
2024-09-10	[Joe Swartz Electric]	play	Link
2024-09-10	[Virginia Dare Extract Co.]	play	Link
2024-09-10	[Southeast Cooler]	play	Link
2024-09-10	[IDF and Mossad agents]	meow	Link
2024-09-10	[rupicard.com]	killsec	Link
2024-09-10	[Vickers Engineering]	akira	Link
2024-09-09	[Controlled Power]	dragonforce	Link
2024-09-09	[Arc-Com]	dragonforce	Link
2024-09-10	[HDI]	bianlian	Link
2024-09-10	[Myelec Electrical]	meow	Link
2024-09-10	[Kadokawa Co Jp]	blacksuit	Link
2024-09-10	[Qeco/coeq]	rhysida	Link
2024-09-10	[E-Z Pack Holdings LLC]	incransom	Link
2024-09-10	[Bank Rakyat]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-06	[americagraphics.com]	ransomhub	Link
2024-09-09	[Pennsylvania State Education Association]	rhysida	Link
2024-09-09	[Anniversary Holding]	bianlian	Link
2024-09-09	[Battle Lumber Co.]	bianlian	Link
2024-09-09	[www.unige.it]	ransomhub	Link
2024-09-09	[Appellation vins fins]	ransomhub	Link
2024-09-07	[www.dpe.go.th]	ransomhub	Link
2024-09-09	[www.bsg.com.au]	ransomhub	Link
2024-09-09	[schynsassurances.be]	killsec	Link
2024-09-09	[pv.be]	killsec	Link
2024-09-09	[Smart Source, Inc.]	bianlian	Link
2024-09-08	[CAM Tyre Trade Systems & Solutions]	qilin	Link
2024-09-06	[▒▒▒▒▒▒▒▒]	cicada3301	Link
2024-09-08	[Stratford School Academy]	rhysida	Link
2024-09-07	[Prosolit]	medusa	Link
2024-09-07	[Grupo Cortefiel]	medusa	Link
2024-09-07	[Nocciole Marchisio]	meow	Link
2024-09-07	[Elsoms Seeds]	meow	Link
2024-09-07	[Millsboro Animal Hospital]	qilin	Link
2024-09-05	[briedis.lt]	ransomhub	Link
2024-09-06	[America Voice]	medusa	Link
2024-09-06	[CK Associates]	bianlian	Link
2024-09-06	[Keya Accounting and Tax Services LLC]	bianlian	Link
2024-09-06	[ctelift.com]	madliberator	Link
2024-09-06	[SESAM Informatics]	hunters	Link
2024-09-06	[riomarineinc.com]	cactus	Link
2024-09-06	[champeau.com]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-05	[cda.be]	killsec	Link
2024-09-05	[belfius.be]	killsec	Link
2024-09-05	[dvv.be]	killsec	Link
2024-09-05	[Custom Security Systems]	hunters	Link
2024-09-05	[Inglenorth.co.uk]	ransomhub	Link
2024-09-05	[cps-k12.org]	ransomhub	Link
2024-09-05	[inorde.com]	ransomhub	Link
2024-09-05	[PhD Services]	dragonforce	Link
2024-09-05	[kawasaki.eu]	ransomhub	Link
2024-09-01	[cbt-gmbh.de]	ransomhub	Link
2024-09-05	[www.towellengineering.net]	ransomhub	Link
2024-09-04	[rhp.com.br]	lockbit3	Link
2024-09-05	[Baird Mandalas Brockstedt LLC]	akira	Link
2024-09-05	[Imetame]	akira	Link
2024-09-05	[SWISS CZ]	akira	Link
2024-09-05	[Cellular Plus]	akira	Link
2024-09-05	[Arch Street Capital Advisors]	qilin	Link
2024-09-04	[Hospital Episcopal San Lucas]	medusa	Link
2024-09-05	[www.parknfly.ca]	ransomhub	Link
2024-09-05	[Western Supplies, Inc]	bianlian	Link
2024-09-04	[Farmers' Rice Cooperative]	play	Link
2024-09-04	[Bakersfield]	play	Link
2024-09-04	[Crain Group]	play	Link
2024-09-04	[Parrish]	blacksuit	Link
2024-09-04	[www.galgorm.com]	ransomhub	Link
2024-09-04	[www.pcipa.com]	ransomhub	Link
2024-09-04	[ych.com]	madliberator	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-03	[idom.com]	lynx	Link
2024-09-04	[plannedparenthood.org]	ransomhub	Link
2024-09-04	[Sunrise Erectors]	hunters	Link
2024-09-03	[simson-maxwell.com]	cactus	Link
2024-09-03	[balboabayresort.com]	cactus	Link
2024-09-03	[flodraulic.com]	cactus	Link
2024-09-03	[mcphillips.co.uk]	cactus	Link
2024-09-03	[rangeramerican.com]	cactus	Link
2024-09-02	[Kingsport Imaging Systems]	medusa	Link
2024-09-02	[Removal.AI]	ransomhub	Link
2024-09-02	[Project Hospitality]	rhysida	Link
2024-09-02	[Shomof Group]	medusa	Link
2024-09-02	[www.sanyo-av.com]	ransomhub	Link
2024-09-01	[Quálitas México]	hunters	Link
2024-09-01	[welland]	trinity	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.