Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241001

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

Web-Config von Seiko-Epson-Geräten ermöglicht Angreifern Übernahme

Das Web-Interface von Geräten wie Druckern von Seiko-Epson ermöglicht Angreifern in vielen Fällen, diese als Administrator zu übernehmen.

- Link

—

CERT-Bund warnt: Mehr als 15.000 Exchange-Server mit Sicherheitslücken

In Deutschland stehen noch immer mehr als 15.000 Exchange-Server mit mindestens einer Codeschmuggel-Lücke offen im Netz, warnt das CERT-Bund.

- Link

—

Monitoring-Software Whatsup Gold: Hersteller rät zum schleunigen Update

Progress warnt, dass teils kritische Sicherheitslücken in Whatsup Gold lauern. Admins sollen so schnell wie möglich aktualisieren.

- Link

—

Kritische Sicherheitslücken: PHP 8.3.12, 8.2.24 und 8.1.30 dichten Lecks ab

Die PHP-Entwickler haben PHP 8.3.12, 8.2.24 und 8.1.30 veröffentlicht. Darin schließen sie mehrere, teils kritische Sicherheitslücken.

- Link

—

Foxit PDF: Manipulierte PDFs können Schadcode durchschleusen

Es sind gegen verschiedene Attacken gerüstete Versionen von Foxit PDF Editor und PDF Reader für macOS und Windows erschienen.

- Link

—

Teils kritische Lücken in Unix-Drucksystem CUPS ermöglichen Codeschmuggel

Im Linux-Drucksystem CUPS wurden teils kritische Sicherheitslücken entdeckt. Angreifer können dadurch etwa Code einschmuggeln.

- Link

—

Schadcode-Schlupfloch in Nvidia Container Toolkit geschlossen

Angreifer können an Sicherheitslücken in Nvidia Container Toolkit und GPU Operator ansetzen, um Systeme zu kompromittieren.

- Link

—

Sicherheitsupdates: DoS-Angriffe auf Cisco-Netzwerkhardware möglich

Aufgrund von mehreren Sicherheitslücken in Ciscos Netzwerkbetriebssystem IOS XE sind verschiedene Geräte verwundbar. Patches stehen zum Download.

- Link

—

Progress Telerik: hochriskante Lücken erlauben Code- und Befehlsschmuggel

In Progress Telerik UI for WPF und WinForms können Angreifer aufgrund von Sicherheitslücken Schadcode und Befehle einschmuggeln.

- Link

—

Teamviewer: Hochriskante Lücken ermöglichen Rechteausweitung

In der Fernwartungssoftware Teamviewer klaffen Sicherheitslücken, durch die Angreifer ihre Rechte ausweiten können. Updates schließen sie.

- 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	0.957580000	0.994820000	Link
CVE-2023-6895	0.927330000	0.990790000	Link
CVE-2023-6553	0.947820000	0.993180000	Link
CVE-2023-6019	0.918710000	0.989950000	Link
CVE-2023-52251	0.949200000	0.993380000	Link
CVE-2023-4966	0.970840000	0.998150000	Link
CVE-2023-49103	0.949680000	0.993480000	Link
CVE-2023-48795	0.964670000	0.996200000	Link
CVE-2023-47246	0.960360000	0.995260000	Link
CVE-2023-46805	0.957170000	0.994750000	Link
CVE-2023-46747	0.971540000	0.998420000	Link
CVE-2023-46604	0.970850000	0.998160000	Link
CVE-2023-4542	0.944110000	0.992630000	Link
CVE-2023-43208	0.974060000	0.999420000	Link
CVE-2023-43177	0.958390000	0.994940000	Link
CVE-2023-42793	0.970970000	0.998220000	Link
CVE-2023-41265	0.907590000	0.989190000	Link
CVE-2023-39143	0.940700000	0.992220000	Link
CVE-2023-38205	0.949280000	0.993390000	Link
CVE-2023-38203	0.964750000	0.996240000	Link
CVE-2023-38146	0.919150000	0.990000000	Link
CVE-2023-38035	0.974550000	0.999660000	Link
CVE-2023-36845	0.967920000	0.997180000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965910000	0.996590000	Link
CVE-2023-35082	0.967900000	0.997170000	Link
CVE-2023-35078	0.971130000	0.998280000	Link
CVE-2023-34993	0.973450000	0.999160000	Link
CVE-2023-34960	0.900520000	0.988760000	Link
CVE-2023-34634	0.923140000	0.990380000	Link
CVE-2023-34362	0.970450000	0.998010000	Link
CVE-2023-34105	0.927500000	0.990820000	Link
CVE-2023-34039	0.943770000	0.992570000	Link
CVE-2023-3368	0.942240000	0.992380000	Link
CVE-2023-33246	0.969870000	0.997800000	Link
CVE-2023-32315	0.971490000	0.998400000	Link
CVE-2023-30625	0.953820000	0.994220000	Link
CVE-2023-30013	0.965950000	0.996600000	Link
CVE-2023-29300	0.967820000	0.997130000	Link
CVE-2023-29298	0.969390000	0.997610000	Link
CVE-2023-28432	0.921930000	0.990270000	Link
CVE-2023-28343	0.937460000	0.991850000	Link
CVE-2023-28121	0.922260000	0.990310000	Link
CVE-2023-27524	0.970600000	0.998060000	Link
CVE-2023-27372	0.974150000	0.999480000	Link
CVE-2023-27350	0.968980000	0.997480000	Link
CVE-2023-26469	0.953540000	0.994160000	Link
CVE-2023-26360	0.964630000	0.996180000	Link
CVE-2023-26035	0.968720000	0.997400000	Link
CVE-2023-25717	0.950620000	0.993610000	Link
CVE-2023-25194	0.964550000	0.996150000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995840000	Link
CVE-2023-24489	0.973150000	0.999030000	Link
CVE-2023-23752	0.952050000	0.993880000	Link
CVE-2023-23333	0.960430000	0.995270000	Link
CVE-2023-22527	0.970500000	0.998030000	Link
CVE-2023-22518	0.959950000	0.995210000	Link
CVE-2023-22515	0.973910000	0.999360000	Link
CVE-2023-21839	0.947720000	0.993160000	Link
CVE-2023-21554	0.952650000	0.994010000	Link
CVE-2023-20887	0.970950000	0.998210000	Link
CVE-2023-1698	0.917150000	0.989810000	Link
CVE-2023-1671	0.962220000	0.995630000	Link
CVE-2023-0669	0.971830000	0.998500000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 30 Sep 2024

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

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

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Verfügbarkeit, Vertraulichkeit und Integrität zu gefährden.

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

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

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Mon, 30 Sep 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 30 Sep 2024

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

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

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um einen Denial of Service Angriff durchzuführen, einen Cross-Site-Scripting-Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Android Patchday August 2022

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen und beliebigen Code auszuführen.

- Link

—

Mon, 30 Sep 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

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Mon, 30 Sep 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Mon, 30 Sep 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 30 Sep 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

—

Mon, 30 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

—

Mon, 30 Sep 2024

[UPDATE] [kritisch] FRRouting Project FRRouting: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Zustand zu erzeugen und potenziell beliebigen Programmcode auszuführen.

- Link

—

Mon, 30 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

—

Mon, 30 Sep 2024

[UPDATE] [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

—

Mon, 30 Sep 2024

[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- Link

—

Fri, 27 Sep 2024

[NEU] [hoch] Hashicorp Vault: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Hashicorp Vault ausnutzen, um seine Privilegien zu erhöhen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/30/2024	[Debian dla-3906 : libwireshark-data - security update]	critical
9/30/2024	[Oracle Linux 7 : freeradius (ELSA-2024-4911)]	critical
9/30/2024	[Rocky Linux 9 : thunderbird (RLSA-2024:6683)]	critical
9/30/2024	[Rocky Linux 9 : firefox (RLSA-2024:6681)]	critical
9/30/2024	[Rocky Linux 8 : kernel-rt (RLSA-2024:7001)]	critical
9/30/2024	[Rocky Linux 9 : expat (RLSA-2024:6754)]	critical
9/30/2024	[Rocky Linux 8 : expat (RLSA-2024:6989)]	critical
9/30/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Flatpak and Bubblewrap vulnerability (USN-7046-1)]	critical
9/30/2024	[SUSE SLES15 Security Update : kernel (Live Patch 1 for SLE 15 SP6) (SUSE-SU-2024:3468-1)]	high
9/30/2024	[Oracle Linux 8 : grafana (ELSA-2024-7349)]	high
9/30/2024	[Oracle Linux 8 / 9 : Unbreakable Enterprise kernel (ELSA-2024-12682)]	high
9/30/2024	[Oracle Linux 9 : cups-filters (ELSA-2024-7346)]	high
9/30/2024	[CentOS 9 : microcode_ctl-20240910-1.el9]	high
9/30/2024	[Oracle Linux 7 : kernel (ELSA-2024-6994)]	high
9/30/2024	[Rocky Linux 9 : fence-agents (RLSA-2024:6726)]	high
9/30/2024	[Rocky Linux 9 : ruby:3.3 (RLSA-2024:6785)]	high
9/30/2024	[Rocky Linux 9 : openssl (RLSA-2024:6783)]	high

Datum	Schwachstelle	Bewertung
9/30/2024	[Rocky Linux 9 : cups-filters (RLSA-2024:7346)]	high
9/30/2024	[Rocky Linux 8 : go-toolset:rhel8 (RLSA-2024:6908)]	high
9/30/2024	[Rocky Linux 9 : libnbd (RLSA-2024:6757)]	high
9/30/2024	[Rocky Linux 9 : golang (RLSA-2024:6913)]	high
9/30/2024	[Rocky Linux 8 : osbuild-composer (RLSA-2024:7262)]	high
9/30/2024	[Rocky Linux 9 : grafana (RLSA-2024:6947)]	high
9/30/2024	[Rocky Linux 8 : python3.12 (RLSA-2024:6961)]	high
9/30/2024	[Rocky Linux 9 : grafana-pcp (RLSA-2024:6946)]	high
9/30/2024	[Rocky Linux 9 : osbuild-composer (RLSA-2024:7204)]	high
9/30/2024	[Rocky Linux 8 : gtk3 (RLSA-2024:6963)]	high
9/30/2024	[Rocky Linux 9 : git-lfs (RLSA-2024:7136)]	high
9/30/2024	[RHEL 8 : grafana (RHSA-2024:7349)]	high
9/30/2024	[RHEL 9 : grafana-pcp (RHSA-2024:7350)]	high
9/30/2024	[RHEL 9 : git-lfs (RHSA-2024:7351)]	high
9/30/2024	[Rocky Linux 8 : git-lfs (RLSA-2024:7135)]	high
9/30/2024	[Rocky Linux 8 : python3 (RLSA-2024:6975)]	high
9/30/2024	[Rocky Linux 8 : ruby:3.3 (RLSA-2024:6784)]	high
9/30/2024	[Debian dla-3907 : lemon - security update]	high
9/30/2024	[Debian dla-3908 : debian-security-support - security update]	high
9/29/2024	[Debian dla-3905 : cups-browsed - security update]	high
10/1/2024	[RHEL 8 : kpatch-patch-4_18_0-553 and kpatch-patch-4_18_0-553_16_1 (RHSA-2024:7429)]	high
10/1/2024	[RHEL 8 : kpatch-patch-4_18_0-372_118_1 and kpatch-patch-4_18_0-372_91_1 (RHSA-2024:7433)]	high
10/1/2024	[RHEL 9 : kpatch-patch-5_14_0-284_52_1 and kpatch-patch-5_14_0-284_79_1 (RHSA-2024:7431)]	high

Datum	Schwachstelle	Bewertung
10/1/2024	[RHEL 8 : kpatch-patch-4_18_0-477_43_1 and kpatch-patch-4_18_0-477_67_1 (RHSA-2024:7430)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 30 Sep 2024

VegaBird Vooki 5.2.9 DLL Hijacking

VegaBird Vooki version 5.2.9 suffers from a dll hijacking vulnerability.

- Link

—

” “Mon, 30 Sep 2024

VegaBird Yaazhini 2.0.2 DLL Hijacking

VegaBird Yaazhini version 2.0.2 suffers from a dll hijacking vulnerability.

- Link

—

” “Mon, 30 Sep 2024

BlackBerry CylanceOPTICS Uninstall Password Bypass

BlackBerry CylanceOPTICS versions prior to 3.3 MR2 and 3.2 MR5 suffer from an uninstall password bypass vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Student Management System 1.0 Insecure Cookie Handling

Student Management System version 1.0 suffers from an insecure cookie handling vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Student Enrollment 1.0 Arbitrary File Upload

Student Enrollment version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Sistem Penyewaan Baju atau Pakaian Berbasis Web 1.0 SQL Injection

Sistem Penyewaan Baju atau Pakaian Berbasis Web version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 30 Sep 2024

Simple Student Quarterly Result / Grade System 1.0 Insecure Settings

Simple Student Quarterly Result / Grade System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Simple Responsive Tourism Website 1.0 Cross Site Request Forgery

Simple Responsive Tourism Website version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 30 Sep 2024

Simple Music Management System 1.0 Add Administrator / Cross Site Request Forgery

Simple Music Management System version 1.0 suffers from add administrator and cross site request forgery vulnerabilities.

- Link

—

” “Mon, 30 Sep 2024

Sample Blog Site 1.0 Cross Site Scripting / Remote File Inclusion

Sample Blog Site version 1.0 suffers from cross site scripting and remote file inclusion vulnerabilities.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Benju.a MVID-2024-0700 Remote Command Execution

Backdoor.Win32.Benju.a malware suffers from a remote command execution vulnerability. This is the 700th release of a malvuln finding.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Prorat.jz MVID-2024-0699 Buffer Overflow

Backdoor.Win32.Prorat.jz malware suffers from a buffer overflow vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Amatu.a MVID-2024-0698 Arbitrary File Write

Backdoor.Win32.Amatu.a malware suffers from a remote arbitrary file write vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Agent.pw MVID-2024-0697 Buffer Overflow

Backdoor.Win32.Agent.pw malware suffers from a buffer overflow vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Backdoor.Win32.Boiling MVID-2024-0696 Code Execution

Backdoor.Win32.Boiling malware suffers from a code execution vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Nexus Repository Traversal Scanner

This scanner helps security enthusiasts to scan for a path traversal vulnerability in Nexus Repository targets in bulk. The scanner will show the number of targets loaded and the state of the current scanning. The URLs will be listed with three status messages: Timeout, Fail, or Success, based on the results.

- Link

—

” “Fri, 27 Sep 2024

Linux OverlayFS Local Privilege Escalation

This Metasploit module exploit targets the Linux kernel bug in OverlayFS. A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel’s OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system.

- Link

—

” “Fri, 27 Sep 2024

Simple Online Banking System 1.0 Insecure Settings

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

- Link

—

” “Fri, 27 Sep 2024

Simple Music Management System 1.0 SQL Injection

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

- Link

—

” “Fri, 27 Sep 2024

Simple College Website 1.0 Shell Upload

Simple College Website version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Simple Chatbot Application 1.0 Insecure Settings

Simple Chatbot Application version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Simbarashe Financial Services 2.9.0 Insecure Direct Object Reference

Simbarashe Financial Services version 2.9.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Seo Panel 4.10.0 Remote File Inclusion

Seo Panel version 4.10.0 suffers from a remote file inclusion vulnerability.

- Link

—

” “Fri, 27 Sep 2024

SchoolPlus 1.0 Insecure Direct Object Reference

SchoolPlus version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Fri, 27 Sep 2024

Sample Blog Site 1.0 Remote File Inclusion

Sample Blog Site version 1.0 suffers from a remote file inclusion vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 27 Sep 2024

ZDI-24-1310: Lenovo Service Bridge Command Injection Remote Code Execution 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: (Okt)

Datum	Opfer	Land	Information
2024-09-27	Agence France-Presse (AFP)	[FRA]	Link
2024-09-27	Smeg	[ITA]	Link
2024-09-27	Richmond Community Schools	[USA]	Link
2024-09-26	University Medical Center (UMC)	[USA]	Link
2024-09-26	CDC Biodiversité	[FRA]	Link
2024-09-26	Aurdel	[SWE]	Link
2024-09-25	Ville de Richardson	[USA]	Link
2024-09-25	Eschau	[FRA]	Link
2024-09-24	Kuwaiti Health Ministry	[KWT]	Link
2024-09-23	VBG Unfallversicherung	[DEU]	Link
2024-09-22	Schumag Aktiengesellschaft	[DEU]	Link
2024-09-22	Arkansas City Water Plant	[USA]	Link
2024-09-22	MoneyGram	[USA]	Link
2024-09-21	Namebay	[MCO]	Link
2024-09-20	Delaware libraries	[USA]	Link
2024-09-19	Fernando Prestes	[BRA]	Link
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
2024-09-15	Technet	[NOR]	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

Datum	Opfer	Land	Information
2024-09-11	Town of Ulster	[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: (Okt)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-30	[datacampos.com]	ElDorado	Link
2024-09-30	[verco.co.uk]	threeam	Link
2024-09-30	[Community Hospital of Anaconda]	meow	Link
2024-09-30	[BELL DATA, Inc]	medusa	Link
2024-09-30	[Travel Alberta]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-30	[IDEALEASE INC]	nitrogen	Link
2024-09-30	[Control Panels USA]	nitrogen	Link
2024-09-30	[Spectrum Industries]	nitrogen	Link
2024-09-30	[Magenta Photo Studio]	nitrogen	Link
2024-09-30	[Brechbuhler Scales Inc]	nitrogen	Link
2024-09-30	[MDSi INC]	nitrogen	Link
2024-09-30	[carlile-group.com]	threeam	Link
2024-09-30	[sacredheart.southwark.sch]	threeam	Link
2024-09-30	[mctas.org.au]	threeam	Link
2024-09-30	[mnpl.com.sg]	threeam	Link
2024-09-30	[canstarrestorations.com]	qilin	Link
2024-09-30	[Lee Hoffoss Injury Lawyers]	meow	Link
2024-09-30	[itap.nacc.go.th]	killsec	Link
2024-09-30	[TOTVS]	blackbyte	Link
2024-09-30	[Keller Williams Realty Group]	qilin	Link
2024-09-30	[McAbee Construction, Inc]	qilin	Link
2024-09-30	[decalesp.com]	blacksuit	Link
2024-09-30	[Isola]	medusa	Link
2024-09-30	[Sub-Zero, Wolf, and Cove]	medusa	Link
2024-09-30	[Plastics Plus]	rhysida	Link
2024-09-30	[Freshstart Credit Repair]	meow	Link
2024-09-30	[MacGillivray Law]	meow	Link
2024-09-19	[weisermemorialhospital.org]	embargo	Link
2024-09-30	[porter.in]	killsec	Link
2024-09-05	[Bayou DeSiard Country Club]	cicada3301	Link
2024-09-29	[poorvika.com]	killsec	Link
2024-09-29	[Affirm Agency]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-29	[InteriorWorx Commercial Flooring]	play	Link
2024-09-29	[Performance Food Centers]	play	Link
2024-09-29	[Reutter]	play	Link
2024-09-29	[4B Components]	play	Link
2024-09-29	[Andantex USA]	play	Link
2024-09-29	[G/S Solutions]	play	Link
2024-09-29	[Condere Ip, Infracom Group]	play	Link
2024-09-29	[The Rubber Resources]	play	Link
2024-09-29	[Classic Business Products]	play	Link
2024-09-29	[Garvey]	play	Link
2024-09-29	[Divine Interprises INC]	incransom	Link
2024-09-29	[DINAS Corp]	incransom	Link
2024-09-29	[Alvan Blanch]	meow	Link
2024-09-26	[cdc-biodiversite.fr]	blackout	Link
2024-09-29	[Moeller Door and Window]	meow	Link
2024-09-29	[OffRoadAction]	meow	Link
2024-09-29	[SaniRent]	meow	Link
2024-09-29	[markdom.com]	ransomhub	Link
2024-09-29	[nfe.fazenda.gov.br]	killsec	Link
2024-09-28	[Soreq NRC]	handala	Link
2024-09-24	[appweb.usinacoruripe.com.br]	ransomhub	Link
2024-09-28	[Røros Hotell]	medusa	Link
2024-09-28	[rockymountaingastro.com]	ransomhub	Link
2024-09-28	[www.contegritygroup.com]	ransomhub	Link
2024-09-27	[PipelBiz.com]	ransomhub	Link
2024-09-28	[Southern Fire Sprinkler]	ciphbit	Link
2024-09-28	[Direct Access Partners]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-27	[infina.vn]	killsec	Link
2024-09-27	[gccustommetal.com]	ElDorado	Link
2024-09-27	[actionfirepros.com]	cactus	Link
2024-09-26	[Xtera Communications]	medusa	Link
2024-09-26	[www.law-taxes.pl]	ransomhub	Link
2024-09-26	[www.tokiwa-group.co.jp]	ransomhub	Link
2024-09-26	[www.careco.se]	ransomhub	Link
2024-09-26	[www.vbrlogistica.com.br]	ransomhub	Link
2024-09-26	[www.naniwa-pump.co.jp]	ransomhub	Link
2024-09-26	[Mile Hi Foods]	play	Link
2024-09-26	[Shenango Area School District]	rhysida	Link
2024-09-23	[KGK Group]	dragonforce	Link
2024-09-23	[Zimmerman & Walsh]	dragonforce	Link
2024-09-25	[kumhotire.com]	lockbit3	Link
2024-09-26	[chcm.us]	lockbit3	Link
2024-09-26	[Schäfer, dein BäckerGmbH & Co. KG]	akira	Link
2024-09-18	[English Construction Company]	lynx	Link
2024-09-26	[lolaliza.com - 250kk]	blacksuit	Link
2024-09-26	[Israel foreign affairs minister Emails]	handala	Link
2024-09-26	[tolsa.com]	abyss	Link
2024-09-23	[DETROIT PBS (PUBLIC TV)]	qilin	Link
2024-09-25	[Concord Management Services]	akira	Link
2024-09-25	[Lawrie Insurance Group]	akira	Link
2024-09-25	[ATG Communications Group]	akira	Link
2024-09-25	[Luso Cuanza]	qilin	Link
2024-09-23	[Hairstore]	medusa	Link
2024-09-23	[IP blue Software Solutions]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-25	[Pennvet.com]	cloak	Link
2024-09-25	[triverus.com]	lynx	Link
2024-09-25	[hindlegroup.com]	cactus	Link
2024-09-25	[kjtait.com]	cactus	Link
2024-09-25	[www.amchar.com]	cactus	Link
2024-09-18	[libraries.delaware.gov]	ransomhub	Link
2024-09-24	[gsdwi.org]	ransomhub	Link
2024-09-24	[PetEdge]	play	Link
2024-09-15	[Bogdan Frasco, LLP]	cicada3301	Link
2024-09-15	[John W. Brooker Co., CPAs]	cicada3301	Link
2024-09-24	[Hughes Gill Cochrane Tinetti]	cicada3301	Link
2024-09-12	[Menninger Clinic]	blacksuit	Link
2024-09-24	[Israel defense minister private photos]	handala	Link
2024-09-24	[cottlesinc.com]	blacksuit	Link
2024-09-24	[Crown Mortgage Company]	cicada3301	Link
2024-09-24	[First Choice Sales & Marketing Group (First Choice)]	bianlian	Link
2024-09-24	[Frigocenter]	arcusmedia	Link
2024-09-24	[Partners Air]	arcusmedia	Link
2024-09-24	[Solutii Sistemas]	arcusmedia	Link
2024-09-24	[Nova Sinseg]	arcusmedia	Link
2024-09-23	[Model Engineering]	cicada3301	Link
2024-09-14	[tellurianinc.org]	ransomhub	Link
2024-09-23	[Kravit, Hovel & Krawczyk SC]	qilin	Link
2024-09-23	[BroadGrain Commodities]	play	Link
2024-09-23	[Eurobulk]	play	Link
2024-09-23	[www.datacampos.com]	ElDorado	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-23	[cucinatagliani.com]	ElDorado	Link
2024-09-23	[cmclb.com]	ElDorado	Link
2024-09-23	[f-t.com]	abyss	Link
2024-09-23	[oleopalma.com.mx]	lockbit3	Link
2024-09-23	[Avi Resort & Casino]	akira	Link
2024-09-23	[medicheck.io]	killsec	Link
2024-09-23	[Benny Gantz]	handala	Link
2024-09-23	[Brown Bottling Group]	akira	Link
2024-09-22	[bakpilic.com.tr]	ransomhub	Link
2024-09-23	[Pureform Radiology Center]	everest	Link
2024-09-23	[Idre Fjäll]	akira	Link
2024-09-23	[Detroit Public TV]	qilin	Link
2024-09-23	[ten8fire.com]	cactus	Link
2024-09-23	[Fabrica Industrial Machinery & Equipment]	trinity	Link
2024-09-23	[Graminex]	dragonforce	Link
2024-09-23	[Canstar Restorations]	qilin	Link
2024-09-22	[hanwa.co.th]	BrainCipher	Link
2024-09-22	[Daughterly Care]	rhysida	Link
2024-09-22	[Woodard , Hernandez , Roth & Day]	qilin	Link
2024-09-20	[savannahcandy.com]	ransomhub	Link
2024-09-21	[Acho.io]	ransomhub	Link
2024-09-20	[Jackson Paper Manufacturing]	play	Link
2024-09-20	[Messe C]	play	Link
2024-09-20	[Noble Environmental]	play	Link
2024-09-20	[Omega Industries]	play	Link
2024-09-20	[Pacific Coast Building Products]	play	Link
2024-09-20	[Thompson Construction Supply]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-20	[Visionary Homes]	incransom	Link
2024-09-20	[KW Realty Group]	qilin	Link
2024-09-20	[Capital Printing]	cicada3301	Link
2024-09-18	[virainsight.com]	ransomhub	Link
2024-09-20	[Juice Generation]	fog	Link
2024-09-20	[River Region Cardiology Associates]	bianlian	Link
2024-09-20	[Greene Acres Nursing Home]	rhysida	Link
2024-09-20	[aroma.com.tr]	ransomhub	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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
2024-09-16	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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
2024-09-03	[www.plumbersstock.com]	ransomhub	Link
2024-09-10	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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
2024-09-15	[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	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-12	[Micron Internet]	medusa	Link
2024-09-12	[TECHNOLOG S.r.l.]	medusa	Link
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
2024-09-12	[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
2024-09-11	[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
2024-09-07	[www.dpe.go.th]	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
2024-09-05	[cda.be]	killsec	Link
2024-09-05	[belfius.be]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-04	[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
2024-09-03	[idom.com]	lynx	Link
2024-09-04	[plannedparenthood.org]	ransomhub	Link
2024-09-04	[Sunrise Erectors]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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.