Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240917

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

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

—

Sicherheitspatch: Gitlab behebt Lücken in Serverversionen

Angreifer konnten Code einschleusen, fremde Konten übernehmen und den Server außer Gefecht setzen. Admins selbst gehosteter Instanzen sollten patchen.

- Link

—

Cisco: DoS- und Rechteausweitungslücken in IOS und weiteren Produkten

In Ciscos IOS und weiteren Produkten klaffen Sicherheitslücken. Angreifer können ihre Rechte ausweiten oder Geräte lahmlegen.

- Link

—

Ivanti: Updates gegen kritische Lecks im Endpoint Manager und weiteren Produkten

Ivanti bessert Schwachstellen in Endpoint Manager, Workspace Control und Cloud Service Appliance aus. Eine Lücke in EPM erreicht die Höchstwertung CVSS 10.

- Link

—

ownCloud: Update stopft teils hochriskante Sicherheitslücken

Das ownCloud-Projekt warnt vor Sicherheitslücken in der Kollaborationssoftware. Angreifer können etwa Zugriff auf Zugangsdaten erlangen.

- Link

—

Citrix Workspace App für Windows ermöglicht Rechteausweitung

In der Citrix Workspace App für Windows klaffen zwei Sicherheitslücken. Angreifer können dadurch ihre Rechte im System ausweiten.

- Link

—

Adobe-Patchday: Kritische Lücken in mehreren Produkten

Adobe stopft am Patchday mehrere kritische Sicherheitslecks. Updates gibt es für acht Produkte des Herstellers.

- Link

—

Patchday Microsoft: Angreifer attackieren vier Lücken in Windows & Co.

Microsoft hat Schwachstellen in unter anderem Azure, SharePoint und Windows geschlossen. Einige Lücken gelten 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	0.994800000	Link
CVE-2023-6895	0.921160000	0.990210000	Link
CVE-2023-6553	0.937150000	0.991840000	Link
CVE-2023-6019	0.918710000	0.989980000	Link
CVE-2023-5360	0.902780000	0.988920000	Link
CVE-2023-52251	0.945480000	0.992840000	Link
CVE-2023-4966	0.970840000	0.998160000	Link
CVE-2023-49103	0.949680000	0.993510000	Link
CVE-2023-48795	0.965330000	0.996500000	Link
CVE-2023-47246	0.961220000	0.995500000	Link
CVE-2023-46805	0.950230000	0.993600000	Link
CVE-2023-46747	0.971020000	0.998260000	Link
CVE-2023-46604	0.969070000	0.997540000	Link
CVE-2023-4542	0.948590000	0.993330000	Link
CVE-2023-43208	0.973740000	0.999290000	Link
CVE-2023-43177	0.961480000	0.995570000	Link
CVE-2023-42793	0.972380000	0.998710000	Link
CVE-2023-41265	0.907590000	0.989220000	Link
CVE-2023-39143	0.936490000	0.991780000	Link
CVE-2023-38205	0.950330000	0.993610000	Link
CVE-2023-38203	0.965830000	0.996640000	Link
CVE-2023-38146	0.920720000	0.990160000	Link
CVE-2023-38035	0.974690000	0.999730000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996900000	Link
CVE-2023-3519	0.965910000	0.996670000	Link
CVE-2023-35082	0.966710000	0.996880000	Link
CVE-2023-35078	0.970930000	0.998200000	Link
CVE-2023-34993	0.973450000	0.999180000	Link
CVE-2023-34960	0.900520000	0.988760000	Link
CVE-2023-34634	0.923140000	0.990400000	Link
CVE-2023-34362	0.970450000	0.997990000	Link
CVE-2023-34039	0.947070000	0.993070000	Link
CVE-2023-3368	0.939780000	0.992160000	Link
CVE-2023-33246	0.967830000	0.997180000	Link
CVE-2023-32315	0.971490000	0.998420000	Link
CVE-2023-30625	0.953610000	0.994210000	Link
CVE-2023-30013	0.965950000	0.996680000	Link
CVE-2023-29300	0.969240000	0.997580000	Link
CVE-2023-29298	0.970810000	0.998130000	Link
CVE-2023-28432	0.920500000	0.990150000	Link
CVE-2023-28343	0.933130000	0.991480000	Link
CVE-2023-28121	0.925430000	0.990630000	Link
CVE-2023-27524	0.970600000	0.998030000	Link
CVE-2023-27372	0.973930000	0.999360000	Link
CVE-2023-27350	0.968480000	0.997340000	Link
CVE-2023-26469	0.953890000	0.994260000	Link
CVE-2023-26360	0.964390000	0.996180000	Link
CVE-2023-26035	0.968440000	0.997330000	Link
CVE-2023-25717	0.954660000	0.994390000	Link
CVE-2023-25194	0.965150000	0.996410000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995910000	Link
CVE-2023-24489	0.973820000	0.999320000	Link
CVE-2023-23752	0.951460000	0.993780000	Link
CVE-2023-23333	0.960430000	0.995320000	Link
CVE-2023-22527	0.970940000	0.998210000	Link
CVE-2023-22518	0.961800000	0.995620000	Link
CVE-2023-22515	0.973160000	0.999080000	Link
CVE-2023-21839	0.951270000	0.993750000	Link
CVE-2023-21554	0.955880000	0.994610000	Link
CVE-2023-20887	0.970840000	0.998150000	Link
CVE-2023-1671	0.962220000	0.995700000	Link
CVE-2023-0669	0.971300000	0.998370000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 16 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

—

Mon, 16 Sep 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 16 Sep 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Mon, 16 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

—

Mon, 16 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, 16 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, 16 Sep 2024

[NEU] [hoch] JetBrains IntelliJ IDEA: Schwachstelle ermöglicht Codeausführung

Ein entfernter Angreifer kann eine Schwachstelle in JetBrains IntelliJ IDEA ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 16 Sep 2024

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in mehreren Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmaßnahmen zu umgehen und Plattform- und Service-Spoofing durchzuführen.

- Link

—

Mon, 16 Sep 2024

[NEU] [hoch] D-LINK Router: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter Angreifer kann mehrere Schwachstellen in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 16 Sep 2024

[UPDATE] [hoch] Adobe ColdFusion: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe ColdFusion ausnutzen, um Informationen offenzulegen oder seine Rechte zu erweitern.

- Link

—

Mon, 16 Sep 2024

[UPDATE] [hoch] GitLab CE/EE: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, beliebigen Code auszuführen, erhöhte Rechte zu erlangen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Mon, 16 Sep 2024

[NEU] [hoch] HP Samsung Universal Print Driver: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in HP Samsung Universal Print Driver ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 13 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

—

Fri, 13 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

—

Fri, 13 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Fri, 13 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

—

Fri, 13 Sep 2024

[UPDATE] [hoch] Apache OFBiz: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache OFBiz ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 13 Sep 2024

[UPDATE] [hoch] Adobe Acrobat Reader: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe Acrobat Reader, Adobe Acrobat, Adobe Acrobat Reader DC und Adobe Acrobat DC ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 13 Sep 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen ausnutzen oder nicht näher beschriebene Auswirkungen zu erzielen.

- Link

—

Fri, 13 Sep 2024

[NEU] [hoch] Kemp LoadMaster: Schwachstelle ermöglicht Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in Kemp LoadMaster ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/16/2024	[Apple iOS < 18 Multiple Vulnerabilities (121250)]	critical
9/16/2024	[Rocky Linux 8 : firefox (RLSA-2024:6682)]	critical
9/16/2024	[Rocky Linux 8 : bubblewrap and flatpak (RLSA-2024:6422)]	critical
9/16/2024	[Rocky Linux 8 : thunderbird (RLSA-2024:6684)]	critical
9/16/2024	[RHEL 9 : thunderbird (RHSA-2024:6683)]	critical
9/16/2024	[RHEL 9 : firefox (RHSA-2024:6681)]	critical
9/16/2024	[RHEL 8 : firefox (RHSA-2024:6682)]	critical
9/16/2024	[RHEL 8 : thunderbird (RHSA-2024:6684)]	critical
9/16/2024	[Sony Network Cameras Stack-based Buffer Overflow (CVE-2018-3938)]	critical
9/15/2024	[Debian dla-3887 : jami - security update]	critical
9/15/2024	[Fedora 39 : bubblewrap / flatpak (2024-03fd821ae2)]	critical
9/16/2024	[Debian dla-3888 : php-twig - security update]	high
9/16/2024	[macOS 13.x < 13.7 Multiple Vulnerabilities (121234)]	high
9/16/2024	[macOS 14.x < 14.7 Multiple Vulnerabilities (121247)]	high
9/16/2024	[Apple iOS < 17.7 Multiple Vulnerabilities (121246)]	high
9/16/2024	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2024-714)]	high

Datum	Schwachstelle	Bewertung
9/16/2024	[Amazon Linux 2023 : microcode_ctl (ALAS2023-2024-716)]	high
9/16/2024	[Debian dla-3889 : python-pymongo-doc - security update]	high
9/16/2024	[RHEL 8 : pcs (RHSA-2024:6670)]	high
9/16/2024	[Rocky Linux 9 : postgresql:16 (RLSA-2024:5929)]	high
9/16/2024	[Rocky Linux 8 : postgresql:16 (RLSA-2024:5927)]	high
9/16/2024	[Rocky Linux 9 : tomcat (RLSA-2024:5693)]	high
9/16/2024	[Rocky Linux 8 : pcs (RLSA-2024:6670)]	high
9/16/2024	[Rocky Linux 9 : postgresql (RLSA-2024:5999)]	high
9/16/2024	[Rocky Linux 8 : libvpx (RLSA-2024:5941)]	high
9/16/2024	[Rocky Linux 8 : tomcat (RLSA-2024:5694)]	high
9/16/2024	[Rocky Linux 8 : postgresql:12 (RLSA-2024:6000)]	high
9/16/2024	[Rocky Linux 9 : kernel (RLSA-2024:6567)]	high
9/16/2024	[RHEL 8 : pcs (RHSA-2024:6702)]	high
9/16/2024	[RHEL 8 : pcs (RHSA-2024:6703)]	high
9/16/2024	[Sony Network Cameras OS Command Injection (CVE-2018-3937)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 16 Sep 2024

VICIdial SQL Injection / Remote Code Execution

Proof of concept exploit that allows an attacker to retrieve administrative credentials through SQL injection and ultimately execute arbitrary code on the target server.

- Link

—

” “Mon, 16 Sep 2024

Rejetto HTTP File Server 2.3m Template Injection / Arbitrary Code Execution

Proof of concept remote code execution exploit for Rejetto HTTP File Server (HFS) version 2.3m.

- Link

—

” “Mon, 16 Sep 2024

Calibre 7.14.0 Remote Code Execution

Proof of concept unauthenticated remote code execution exploit for Calibre versions 7.14.0 and below.

- Link

—

” “Mon, 16 Sep 2024

Veeam Backup And Replication 12.1.2.172 Remote Code Execution

Veeam Backup and Replication version 12.1.2.172 unauthenticated remote code execution exploit.

- Link

—

” “Mon, 16 Sep 2024

Ship Ferry Ticket Reservation System 1.0 SQL Injection

Ship Ferry Ticket Reservation System version 1.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

” “Mon, 16 Sep 2024

Reservation Management System 1.0 Cross Site Request Forgery

Reservation Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 16 Sep 2024

Online Job Recruitment Portal Project 1.0 Arbitrary File Upload

Online Job Recruitment Portal Project version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Mon, 16 Sep 2024

IFSC Code Finder Portal 1.0 Insecure Settings

IFSC Code Finder Portal version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 16 Sep 2024

GYM Management System 1.0 Insecure Settings

GYM Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 16 Sep 2024

Emergency Ambulance Hiring Portal 1.0 SQL Injection

Emergency Ambulance Hiring Portal version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 16 Sep 2024

ManageEngine DeviceExpert 5.9.7 Build 5970 Hash Disclosure

ManageEngine DeviceExpert version 5.9.7 build 5970 allows for usernames and salted MD5 password hashes to be disclosed.

- Link

—

” “Mon, 16 Sep 2024

COVID19 Testing Management System 1.0 Insecure Settings

COVID19 Testing Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 16 Sep 2024

BP Monitoring Management System 1.0 SQL Injection

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

- Link

—

” “Mon, 16 Sep 2024

Auto/Taxi Stand Management System 1.0 SQL Injection

Auto/Taxi Stand Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Fri, 13 Sep 2024

Ivanti EPM Remote Code Execution

Proof of concept remote code execution exploit for Ivanti EPM versions prior to 2022 SU6 or the 2024 September update.

- Link

—

” “Fri, 13 Sep 2024

GeoServer Remote Code Execution

Proof of concept remote code execution exploit for GeoServer versions prior 2.23.6, 2.24.4, and 2.25.2.

- Link

—

” “Fri, 13 Sep 2024

Webpay E-Commerce 1.0 Cross Site Scripting

Webpay E-Commerce version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Men Salon Management System 2.0 PHP Code Injection

Men Salon Management System version 2.0 suffers from a php code injection vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Emergency Ambulance Hiring Portal 1.0 Insecure Settings

Emergency Ambulance Hiring Portal version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Car Washing Management System 1.0 Insecure Settings

Car Washing Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Bus Pass Management System 1.0 Insecure Settings

Bus Pass Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 13 Sep 2024

BP Monitoring Management System 1.0 Insecure Settings

BP Monitoring Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 13 Sep 2024

Beauty Parlour And Saloon Management System 1.1 Insecure Cookie Handling

Beauty Parlour and Saloon Management System version 1.1 suffers from an insecure cooking handling vulnerability.
- Link
—
” “Fri, 13 Sep 2024
Auto/Taxi Stand Management System 1.0 PHP Code Injection
Auto/Taxi Stand Management System version 1.0 suffers from a php code injection vulnerability.
- Link
—
” “Fri, 13 Sep 2024
Art Gallery Management System 1.0 Insecure Settings
Art Gallery Management System version 1.0 suffers from an ignored default credential vulnerability.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Fri, 13 Sep 2024
ZDI-24-1226: mySCADA myPRO Hard-Coded Credentials Remote Code Execution Vulnerability
- Link
—
” “Fri, 13 Sep 2024
ZDI-24-1225: SolarWinds Access Rights Manager Hard-Coded Credentials Authentication Bypass Vulnerability
- Link
—
” “Fri, 13 Sep 2024
ZDI-24-1224: SolarWinds Access Rights Manager JsonSerializationBinder Deserialization of Untrusted Data 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: (Sep)

Datum	Opfer	Land	Information
2024-09-15	Radio Geretsried	[DEU]	Link
2024-09-12	▯▯▯▯▯▯ (Kantsu)	[JPN]	Link
2024-09-12	LolaLiza	[BEL]	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
2024-09-02	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
2024-09-16	[Cruz Marine (cruz.local)]	lynx	Link
2024-09-16	[SuperCommerce.ai]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-09-10	[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
2024-09-10	[City of Pleasanton, California]	ValenciaLeaks	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
2024-09-06	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-11	[Charles Darwin School]	blacksuit	Link
2024-09-11	[S. Walter Packaging]	fog	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-10	[E-Z Pack Holdings LLC]	incransom	Link
2024-09-10	[Bank Rakyat]	hunters	Link
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	[cardiovirginia.com]	ransomhub	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.