Cybersecurity Morgenreport

Ausgabe: 20231207

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

Security-News

Heise - Security-Alert

Zehn Sicherheitslücken in aktueller Chrome-Version geschlossen
Angreifer können Googles Webbrowser Chrome attackieren. Aktualisierte Versionen schaffen Abhilfe.
- Link

—

Codeschmuggel in Atlassian-Produkten: Vier kritische Lücken aufgetaucht
Admins von Confluence, Jira und Bitbucket kommen aus dem Patchen nicht heraus: Erneut hat Atlassian dringende Updates für seine wichtigsten Produkte vorgelegt.
- Link

—

Patchday Android: Android 11, 12, 13 und 14 für Schadcode-Attacken anfällig
Angreifer können Android-Smartphones und -Tablets verschiedener Hersteller ins Visier nehmen. Für einige Geräte gibt es Sicherheitsupdates.
- Link

—

Neue Squid-Version behebt Denial-of-Service-Lücken
Drei Sicherheitsprobleme können dazu führen, dass der freie Web-Proxy Squid seinen Dienst verweigert. Admins sollten die bereitstehenden Updates einpflegen.
- Link

—

Sicherheitsupdates: Angreifer können Zyxel-NAS mit präparierten URLs attackieren
Zwei NAS-Modelle von Zyxel sind verwundbar. In aktuellen Versionen haben die Entwickler mehrere kritische Sicherheitslücken geschlossen.
- Link

—

Entwicklungsplattform: Neue GitLab-Versionen beheben zehn Sicherheitslücken
Neben Cross-Site-Scripting und Rechteproblemen beheben die neuen Versionen der Versionsverwaltung auch DoS-Lücken. Das GitLab-Team empfiehlt ein Update.
- Link

—

Sicherheitsupdate: Verwundbare Komponenten gefährden Nessus Network Monitor
Schwachstellen unter anderem in OpenSSL gefährden die Monitoringlösung Nessus Network Monitor.
- Link

—

Sicherheitspatch verfügbar: Kritische Lücke in VMware Cloud Director behoben
In bestimmten Fällen können Angreifer VMware Cloud Director attackieren. Nach einem Workaround gibt es nun einen Sicherheitspatch.
- Link

—

Support ausgelaufen: Mehr als 20.000 Exchange Server potenziell angreifbar
Sicherheitsforscher sind unter anderem in Europa auf tausende Exchange Server gestoßen, die EOL sind.
- Link

—

Apache ActiveMQ: Mehrere Codeschmuggel-Lücken von Botnetbetreibern ausgenutzt
Die im Oktober veröffentlichten kritischen Sicherheitsprobleme in ActiveMQ nützen nun Botnet-Betreibern. Derweil gibt es ein neues Sicherheitsproblem.
- Link

—

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.

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.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-5360	0.967980000	0.995970000	Link
CVE-2023-4966	0.922670000	0.987190000	Link
CVE-2023-46747	0.965530000	0.995040000	Link
CVE-2023-46604	0.968050000	0.995990000	Link
CVE-2023-42793	0.972640000	0.998150000	Link
CVE-2023-38035	0.970940000	0.997220000	Link
CVE-2023-35078	0.958120000	0.992850000	Link
CVE-2023-34362	0.928450000	0.987940000	Link
CVE-2023-34039	0.929570000	0.988070000	Link
CVE-2023-33246	0.971220000	0.997360000	Link
CVE-2023-32315	0.961510000	0.993660000	Link
CVE-2023-30625	0.936230000	0.988880000	Link
CVE-2023-30013	0.936180000	0.988870000	Link
CVE-2023-28771	0.918550000	0.986710000	Link
CVE-2023-27524	0.906990000	0.985450000	Link
CVE-2023-27372	0.971560000	0.997540000	Link
CVE-2023-27350	0.972290000	0.997960000	Link
CVE-2023-26469	0.933320000	0.988540000	Link
CVE-2023-26360	0.934340000	0.988690000	Link
CVE-2023-25717	0.962820000	0.994040000	Link
CVE-2023-25194	0.904410000	0.985250000	Link
CVE-2023-2479	0.958820000	0.993020000	Link
CVE-2023-24489	0.969450000	0.996580000	Link
CVE-2023-22518	0.967630000	0.995870000	Link
CVE-2023-22515	0.955290000	0.992190000	Link
CVE-2023-21839	0.956630000	0.992510000	Link
CVE-2023-21823	0.955130000	0.992130000	Link
CVE-2023-21554	0.961220000	0.993580000	Link
CVE-2023-20887	0.952390000	0.991590000	Link
CVE-2023-1671	0.950520000	0.991150000	Link
CVE-2023-0669	0.966690000	0.995440000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 06 Dec 2023

[NEU] [hoch] Atlassian Produkte: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Atlassian Bitbucket, Atlassian Confluence und Atlassian Jira Software ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 06 Dec 2023
[NEU] [hoch] Extreme Networks IQ Engine: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Extreme Networks IQ Engine ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] Red Hat Quarkus: Schwachstelle ermöglicht die Umgehung von Sicherheitsmaßnahmen oder die Verursachung eines Denial-of-Service-Zustands
Ein entfernter anonymer Angreifer kann eine Schwachstelle in Red Hat Quarkus ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] Samsung Android: Mehrere Schwachstellen ermöglichen
Ein entfernter Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder Dateien zu manipulieren.
- Link

—

Wed, 06 Dec 2023
[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen
Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Wed, 06 Dec 2023

[UPDATE] [hoch] Google Android: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.
- Link

—

Tue, 05 Dec 2023
[UPDATE] [hoch] Tenable Security Nessus Network Monitor: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Tenable Security Nessus Network Monitor ausnutzen, um vertrauliche Informationen offenzulegen, beliebigen Code auszuführen oder Dateien zu manipulieren.
- Link

—

Tue, 05 Dec 2023
[UPDATE] [hoch] GitLab: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren, seine Berechtigungen zu erweitern oder XSS-Angriffe durchzuführen.
- Link

—

Tue, 05 Dec 2023
[NEU] [hoch] Samsung Android: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder Sicherheitsmaßnahmen zu umgehen.
- Link

—

Tue, 05 Dec 2023
[NEU] [hoch] Microsoft Azure RTOS NetX: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Azure RTOS NetX ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Tue, 05 Dec 2023
[NEU] [hoch] IBM Informix: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in IBM Informix ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.
- Link

—

Tue, 05 Dec 2023
[UPDATE] [hoch] PHP: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen, Dateien zu manipulieren und beliebigen Programmcode mit den Rechten des Dienstes ausführen zu können.
- Link

—

Tue, 05 Dec 2023
[UPDATE] [hoch] Perl: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode mit den Rechten des Dienstes
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Perl ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen oder einen Denial of Service Angriff durchzuführen.
- Link

—

Tue, 05 Dec 2023
[UPDATE] [hoch] GNU Mailman: Mehrere Schwachstellen
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in GNU Mailman ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen und Adminrechte zu erhalten.
- Link

—

Tue, 05 Dec 2023
[UPDATE] [hoch] PHP: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programm-

code auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/7/2023	[openSUSE 15 Security Update : frr (SUSE-SU-2023:4663-1)]	critical
12/6/2023	[OwnCloud 10.6.x < 10.13.1 WebDav Authentication Bypass]	critical
12/6/2023	[Atlassian Confluence 4.x < 7.19.17 Template Injection]	critical
12/6/2023	[Atlassian Confluence 8.x < 8.4.5 Template Injection]	critical
12/6/2023	[Atlassian Confluence 8.5.x < 8.5.4 Template Injection]	critical
12/6/2023	[Atlassian Confluence 8.6.x < 8.6.2 Template Injection]	critical
12/6/2023	[Atlassian Confluence 8.7.x < 8.7.1 Template Injection]	critical
12/6/2023	[RHEL 8 : squid:4 (RHSA-2023:7668)]	critical
12/6/2023	[Rocky Linux 8 : squid:4 (RLSA-2023:7668)]	critical
12/5/2023	[Fedora 39 : perl / perl-Devel-Cover / perl-PAR-Packer / polymake (2023-c67f4dbf13)]	critical
12/5/2023	[Ubuntu 16.04 ESM : Linux kernel vulnerabilities (USN-6532-1)]	critical
12/7/2023	[openSUSE 15 Security Update : qemu (SUSE-SU-2023:4662-1)]	high
12/7/2023	[openSUSE 15 Security Update : suse-build-key (SUSE-SU-2023:4672-1)]	high
12/6/2023	[Apache Tomcat 10.1.0-M1 < 10.1.16 Request Smuggling]	high
12/6/2023	[Apache Tomcat 9.0.0-M1 < 9.0.83 Request Smuggling]	high
12/6/2023	[Apache Tomcat 8.5.x < 8.5.96 Request Smuggling]	high
12/6/2023	[Appwrite < 1.4.0 Server-Side Request Forgery]	high
12/6/2023	[Ubuntu 16.04 ESM / 18.04 ESM : Open VM Tools vulnerabilities (USN-6463-2)]	high
12/6/2023	[Ubuntu 22.04 LTS / 23.10 : Linux kernel vulnerabilities (USN-6536-1)]	high
12/6/2023	[VMware Tools for Linux 10.3.x < 10.3.26 Authentication Bypass (VMSA-2023-0019)]	high
12/6/2023	[WordPress 6.0 < 6.4.2]	high
12/6/2023	[RHEL 8 : postgresql:12 (RHSA-2023:7667)]	high
12/6/2023	[RHEL 8 : postgresql:12 (RHSA-2023:7666)]	high
12/6/2023	[Ubuntu 23.10 : Linux kernel (GCP) vulnerabilities (USN-6537-1)]	high
12/6/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : PostgreSQL vulnerabilities (USN-6538-1)]	high
12/6/2023	[macOS 14.x < 14.1.2 Multiple Vulnerabilities (HT214032)]	high
12/6/2023	[Fedora 38 : llhttp / python-aiohttp / uxplay (2023-bc1f081ca0)]	high
12/6/2023	[Fedora 39 : llhttp / python-aiohttp / uxplay (2023-5130a73b00)]	high
12/6/2023	[Fedora 39 : gmailctl (2023-e3e4e3f51a)]	high
12/6/2023	[Fedora 38 : gmailctl (2023-6f4c5b6331)]	high
12/6/2023	[Rocky Linux 8 : postgresql:13 (RLSA-2023:7581)]	high
12/6/2023	[Rocky Linux 8 : kernel (RLSA-2023:7549)]	high
12/6/2023	[Rocky Linux 8 : kernel-rt (RLSA-2023:7548)]	high
12/5/2023	[Fedora 38 : clevis-pin-tpm2 / keyring-ima-signer / libkrun / rust-bodhi-cli / etc (2023-6215ea423b)]	high
12/5/2023	[FreeBSD : FreeBSD – TCP spoofing vulnerability in pf(4) (9cbbc506-93c1-11ee-8e38-002590c1f29c)]	high
12/5/2023	[Ubuntu 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6534-1)]	high
12/5/2023	[Ubuntu 22.04 LTS : Linux kernel (OEM) vulnerabilities (USN-6533-1)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Wed, 06 Dec 2023
Winter CMS 1.2.2 Server-Side Template Injection
Winter CMS version 1.2.2 suffers from a server-side template injection vulnerability.
- Link
—
” “Wed, 06 Dec 2023
CE Phoenixcart 1.0.8.20 Shell Upload
CE Phoenixcart version 1.0.8.20 suffers from a remote shell upload vulnerability.
- Link
—
” “Tue, 05 Dec 2023
FortiWeb VM 7.4.0 build577 CLI Crash
FortiWeb VM version 7.4.0 build577 suffers from a post authentication CLI crash when provided a long password.
- Link
—
” “Mon, 04 Dec 2023
TinyDir 1.2.5 Buffer Overflow
TinyDir versions 1.2.5 and below suffer from a buffer overflow vulnerability with long path names.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Appointment Scheduler 3.0 CSV Injection
PHPJabbers Appointment Scheduler version 3.0 suffers from a CSV injection vulnerability.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Appointment Scheduler 3.0 Missing Rate Limiting
PHPJabbers Appointment Scheduler version 3.0 suffers from a missing rate limiting control that can allow for resource exhaustion.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Appointment Scheduler 3.0 Cross Site Scripting
PHPJabbers Appointment Scheduler version 3.0 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Appointment Scheduler 3.0 HTML Injection
PHPJabbers Appointment Scheduler version 3.0 suffers from multiple html injection vulnerabilities.
- Link
—
” “Mon, 04 Dec 2023
October CMS 3.4.0 Wiki Article Cross Site Scripting
October CMS version 3.4.0 suffers from a persistent cross site scripting vulnerability when a user has article posting capabilities.
- Link
—
” “Mon, 04 Dec 2023
October CMS 3.4.0 Category Cross Site Scripting
October CMS version 3.4.0 suffers from a persistent cross site scripting vulnerability when a user has category-creating capabilities.
- Link
—
” “Mon, 04 Dec 2023
October CMS 3.4.0 Blog Cross Site Scripting

October CMS version 3.4.0 suffers from a persistent cross site scripting vulnerability when a user has blog-creating capabilities.
- Link
—
” “Mon, 04 Dec 2023
October CMS 3.4.0 Author Cross Site Scripting
October CMS version 3.4.0 suffers from a persistent cross site scripting vulnerability when a user has author posting capabilities.
- Link
—
” “Mon, 04 Dec 2023
October CMS 3.4.0 About Cross Site Scripting
October CMS version 3.4.0 suffers from a persistent cross site scripting vulnerability where a user has the ability to edit the landing/about page.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Car Rental 3.0 HTML Injection
PHPJabbers Car Rental version 3.0 suffers from an html injection vulnerability.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Car Rental 3.0 Cross Site Scripting
PHPJabbers Car Rental version 3.0 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Car Rental 3.0 CSV Injection
PHPJabbers Car Rental version 3.0 suffers from a CSV injection vulnerability.
- Link
—
” “Mon, 04 Dec 2023
R Radio Network FM Transmitter 1.07 system.cgi Password Disclosure
R Radio Network FM Transmitter version 1.07 suffers from an improper access control that allows an unauthenticated actor to directly reference the system.cgi endpoint and disclose the clear-text password of the admin user allowing authentication bypass and FM station setup access.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Car Rental 3.0 Missing Rate Limit
PHPJabbers Car Rental version 3.0 suffers from a missing rate limiting control that can allow for resource exhaustion.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Time Slots Booking Calendar 4.0 Missing Rate Limiting
PHPJabbers Time Slots Booking Calendar version 4.0 suffers from a missing rate limiting control that can allow for resource exhaustion.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Availability Booking Calendar 5.0 Missing Rate Limiting
PHPJabbers Availability Booking Calendar version 5.0 suffers from a missing rate limiting control that can allow for resource exhaustion.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Shuttle Booking Software 2.0 CSV Injection
PHPJabbers Shuttle Booking Software version 2.0 suffers from a CSV injection vulnerability.
- Link
—

” “Mon, 04 Dec 2023
PHPJabbers Time Slots Booking Calendar 4.0 Cross Site Scripting
PHPJabbers Time Slots Booking Calendar version 4.0 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Time Slots Booking Calendar 4.0 HTML Injection
PHPJabbers Time Slots Booking Calendar version 4.0 suffers from an html injection vulnerability.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Time Slots Booking Calendar 4.0 CSV Injection
PHPJabbers Time Slots Booking Calendar version 4.0 suffers from a CSV injection vulnerability.
- Link
—
” “Mon, 04 Dec 2023
PHPJabbers Availability Booking Calendar 5.0 HTML Injection
PHPJabbers Availability Booking Calendar version 5.0 suffers from an html injection vulnerability.
- Link
—
”

0-Days der letzten 5 Tage

“Tue, 05 Dec 2023
ZDI-23-1762: SolarWinds Orion Platform VimChartInfo SQL Injection Remote Code Execution Vulnerability
- Link
—
” “Tue, 05 Dec 2023
ZDI-23-1761: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 05 Dec 2023
ZDI-23-1760: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 05 Dec 2023
ZDI-23-1759: Adobe Acrobat Reader DC Font Parsing Use-After-Free Remote Code Execution Vulnerability
- Link
—
” “Tue, 05 Dec 2023
ZDI-23-1758: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Tue, 05 Dec 2023
ZDI-23-1757: Adobe Acrobat Reader DC Font Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability
- Link
—
”

Die Hacks der Woche

mit Martin Haunschmid

Eine Zeitreise in die Anfänge des hack-for-hire

Zum Youtube Video

Cyberangriffe: (Dez)

Datum	Opfer	Land	Information
2023-12-06	Nissan Oceania	[AUS]	Link
2023-12-05	Dameron Hospital	[USA]	Link
2023-12-05	Gräbener Maschinentechnik	[DEU]	Link
2023-12-04	Caribbean Community (Caricom) Secretariat	[GUY]	Link

Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-07	[Tryax Realty Management - Press Release]	monti	Link
2023-12-06	[Campbell County Schools]	medusa	Link
2023-12-06	[Deutsche Energie-Agentur]	alphv	Link
2023-12-06	[Compass Group Italia]	akira	Link
2023-12-06	[Aqualectra Holdings]	akira	Link
2023-12-06	[Acero Engineering]	bianlian	Link
2023-12-06	[syrtech.com]	threeam	Link
2023-12-06	[ACCU Reference Medical Lab]	medusa	Link
2023-12-06	[Sagent]	medusa	Link
2023-12-06	[fpz.com]	lockbit3	Link
2023-12-06	[labelians.fr]	lockbit3	Link
2023-12-06	[polyclinique-cotentin.com]	lockbit3	Link
2023-12-06	[Lischkoff and Pitts, P.C.]	8base	Link
2023-12-06	[SMG Confrere]	8base	Link
2023-12-06	[Calgary TELUS Convention Centre]	8base	Link
2023-12-06	[astley.]	8base	Link
2023-12-05	[Henry Schein Inc - Henry's " LOST SHINE "]	alphv	Link
2023-12-05	[TraCS Florida FSU]	alphv	Link
2023-12-05	[aldoshoes.com]	lockbit3	Link
2023-12-05	[laprensani.com]	lockbit3	Link
2023-12-05	[mapc.org]	lockbit3	Link
2023-12-05	[ussignandmill.com]	threeam	Link
2023-12-05	[Rudolf-Venture Chemical Inc - Part 1]	monti	Link
2023-12-05	[Akumin]	bianlian	Link
2023-12-05	[CLATSKANIEPUD]	alphv	Link
2023-12-05	[restargp.com]	lockbit3	Link
2023-12-05	[concertus.co.uk]	abyss	Link
2023-12-05	[Bowden Barlow Law PA]	medusa	Link
2023-12-05	[Rosens Diversified Inc]	medusa	Link
2023-12-05	[Henry County Schools]	blacksuit	Link
2023-12-05	[fps.com]	blacksuit	Link
2023-12-04	[Full access to the school network USA]	everest	Link
2023-12-04	[CMS Communications]	qilin	Link
2023-12-04	[Tipalti]	alphv	Link
2023-12-04	[Great Lakes Technologies]	qilin	Link
2023-12-04	[Midea Carrier]	akira	Link
2023-12-04	[ychlccsc.edu.hk]	lockbit3	Link
2023-12-04	[nlt.com]	blackbasta	Link
2023-12-04	[Getrix]	akira	Link
2023-12-04	[Evnhcmc]	alphv	Link
2023-12-03	[mirle.com.tw]	lockbit3	Link
2023-12-03	[Bern Hotels & Resorts]	akira	Link
2023-12-03	[Tipalti claimed as a victim - but we'll extort Roblox and Twitch, two of their affected cl]	alphv	Link
2023-12-03	[Tipalti claimed as a victim - but we'll extort Roblox, one of their affected clients, indi]	alphv	Link
2023-12-02	[Lisa Mayer CA, Professional Corporation]	alphv	Link
2023-12-02	[bboed.org]	lockbit3	Link
2023-12-01	[hnncsb.org]	lockbit3	Link
2023-12-01	[elsewedyelectric.com]	lockbit3	Link
2023-12-01	[Austal USA]	hunters	Link
2023-12-02	[inseinc.com]	blackbasta	Link
2023-12-02	[royaleinternational.com]	alphv	Link
2023-12-01	[Dörr Group]	alphv	Link
2023-12-01	[IRC Engineering]	alphv	Link
2023-12-01	[Hello Cristina from Law Offices of John E Hill]	monti	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-12-01	[Hello Jacobs from RVC]	monti	Link
2023-12-01	[Austal]	hunters	Link
2023-12-01	[St. Johns River Water Management District]	hunters	Link
2023-12-01	[Kellett & Bartholow PLLC]	incransom	Link
2023-12-01	[Centroedile Milano]	blacksuit	Link
2023-12-01	[Iptor]	akira	Link
2023-12-01	[farwickgrote.de]	cloak	Link
2023-12-01	[skncustoms.com]	cloak	Link
2023-12-01	[euro2000-spa.it]	cloak	Link
2023-12-01	[Thenewtrongroup.com]	cloak	Link
2023-12-01	[Bankofceylon.co.uk]	cloak	Link
2023-12-01	[carranza.on.ca]	cloak	Link
2023-12-01	[Agamatrix]	meow	Link

Quellen

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

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.