Cybersecurity Morgenreport

Ausgabe: 20231205

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

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

—

Sicherheitslücke in Hikvision-Kameras und NVR ermöglicht unbefugten Zugriff
Verschiedene Modelle des chinesischen Herstellers gestatteten Angreifern den unbefugten Zugriff. Auch andere Marken sind betroffen, Patches stehen bereit.
- Link

—

Sicherheitslücke: Schadcode-Attacken auf Solarwinds Platform möglich
Die Solarwinds-Entwickler haben zwei Schwachstellen in ihrer Monitoringsoftware geschlossen.
- Link

—

Scans zu kritischer Sicherheitslücke in ownCloud-Plugin
Die Schwachstelle im GraphAPI-Plugin kann zur unfreiwilligen Preisgabe der Admin-Zugangsdaten führen. ownCloud-Admins sollten schnell reagieren.
- Link

—

Jetzt patchen! Attacken auf Google Chrome
Der Webbrowser Chrome ist verwundbar. Die Entwickler haben mehrere Schwachstellen geschlossen.
- 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	0.995950000	Link
CVE-2023-4966	0.922670000	0.987090000	Link
CVE-2023-46747	0.965530000	0.995020000	Link
CVE-2023-46604	0.968050000	0.995980000	Link
CVE-2023-42793	0.972640000	0.998140000	Link
CVE-2023-38035	0.970940000	0.997210000	Link
CVE-2023-35078	0.958120000	0.992800000	Link
CVE-2023-34362	0.928450000	0.987850000	Link
CVE-2023-34039	0.925730000	0.987540000	Link
CVE-2023-33246	0.971220000	0.997330000	Link
CVE-2023-32315	0.961510000	0.993640000	Link
CVE-2023-30625	0.936230000	0.988820000	Link
CVE-2023-30013	0.936180000	0.988810000	Link
CVE-2023-28771	0.918550000	0.986610000	Link
CVE-2023-27524	0.906990000	0.985370000	Link
CVE-2023-27372	0.971560000	0.997520000	Link
CVE-2023-27350	0.972290000	0.997960000	Link
CVE-2023-26469	0.933320000	0.988450000	Link
CVE-2023-26360	0.934340000	0.988620000	Link
CVE-2023-25717	0.962820000	0.994010000	Link
CVE-2023-25194	0.910980000	0.985770000	Link
CVE-2023-2479	0.958820000	0.992980000	Link
CVE-2023-24489	0.969450000	0.996580000	Link
CVE-2023-22518	0.967630000	0.995850000	Link
CVE-2023-22515	0.955290000	0.992140000	Link
CVE-2023-21839	0.956630000	0.992460000	Link
CVE-2023-21823	0.955130000	0.992090000	Link
CVE-2023-21554	0.961220000	0.993560000	Link
CVE-2023-20887	0.952390000	0.991540000	Link
CVE-2023-1671	0.950520000	0.991120000	Link
CVE-2023-0669	0.966690000	0.995420000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 04 Dec 2023

[NEU] [UNGEPATCHT] [hoch] Logback: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Mon, 04 Dec 2023
[NEU] [hoch] Squid: Mehrere Schwachstellen ermöglichen Denial of Service
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Mon, 04 Dec 2023
[UPDATE] [hoch] PCRE (Perl Compatible Regular Expressions): Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PCRE (Perl Compatible Regular Expressions) ausnutzen, um einen Denial of Service Angriff durchzuführen und um Informationen offen zu legen.
- Link

—

Mon, 04 Dec 2023
[UPDATE] [hoch] zlib: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in zlib ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Mon, 04 Dec 2023
[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

Mon, 04 Dec 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Mon, 04 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

—

Mon, 04 Dec 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung
Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 04 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

—

Mon, 04 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

—

Mon, 04 Dec 2023
[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla 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, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Mon, 04 Dec 2023
[NEU] [hoch] Logback: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Fri, 01 Dec 2023
[UPDATE] [hoch] SHA-3 Implementierungen: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in den SHA-3 Implementierungen mehrerer Produkte ausnutzen, um beliebigen Programmcode auszuführen kryptographische Eigenschaften einzuschränken.
- Link

—

Fri, 01 Dec 2023
[UPDATE] [hoch] Xerox FreeFlow Print Server: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Print Server ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität des Systems zu gefährden.
- Link

—

Fri, 01 Dec 2023
[UPDATE] [hoch] Arcserve Unified Data Protection: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Arcserve Unified Data Protection ausnutzen, um beliebigen Code auszuführen, Dateien zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.
- Link

—

Fri, 01 Dec 2023
[NEU] [hoch] Apple Safari: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Apple Safari ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.
- Link

—

Fri, 01 Dec 2023
[NEU] [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

—

Fri, 01 Dec 2023
[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Fri, 01 Dec 2023
[UPDATE] [hoch] Red Hat OpenStack Platform : Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in der Red Hat OpenStack Platform ausnutzen, um seine Privilegien zu erhöhen, einen Denial of Service zu verursachen oder Informationen offenzulegen.
- Link

—

Fri, 01 Dec 2023
[NEU] [hoch] Apple macOS: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Code auszuführen oder um vertrauliche Informationen offenzulegen.
- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/4/2023	[Debian DLA-3675-1 : zbar - LTS security update]	critical
12/1/2023	[OwnCloud graphapi 0.2.x < 0.2.1 / 0.3.x < 0.3.1 Sensitive Informations Disclosure]	critical
12/1/2023	[FreeBSD : electron25 – multiple vulnerabilities (302fc846-860f-482e-a8f6-ee9f254dfacf)]	critical
12/1/2023	[FreeBSD : electron26 – multiple vulnerabilities (7e1a508f-7167-47b0-b9fc-95f541933a86)]	critical
12/1/2023	[openSUSE 15 Security Update : chromium (openSUSE-SU-2023:0387-1)]	critical
12/1/2023	[Apache Superset < 2.1.0 Secure Session Key]	critical
12/1/2023	[Debian DLA-3679-1 : vlc - LTS security update]	critical
12/1/2023	[Debian DSA-5569-1 : chromium - security update]	critical
12/4/2023	[Trellix Enterprise Security Manager < 11.6.7 Command Injection]	high
12/4/2023	[ManageEngine NetFlow Analyzer 12.5.x < 12.5.657 / 12.6.x < 12.6.002 / 12.6.104 / 12.6.118 Authenticate Bypass]	high
12/4/2023	[RHEL 7 : rh-mariadb105-galera and rh-mariadb105-mariadb (RHSA-2023:7633)]	high
12/4/2023	[Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Request Tracker vulnerabilities (USN-6529-1)]	high
12/4/2023	[RHEL 7 : Red Hat JBoss Enterprise Application Platform 7.4.14 on RHEL 7 (RHSA-2023:7637)]	high
12/4/2023	[RHEL 8 : Red Hat JBoss Enterprise Application Platform 7.4.14 on RHEL 8 (RHSA-2023:7638)]	high
12/4/2023	[RHEL 9 : Red Hat JBoss Enterprise Application Platform 7.4.14 on RHEL 9 (RHSA-2023:7639)]	high
12/3/2023	[Debian DLA-3681-1 : amanda - LTS security update]	high
12/3/2023	[Debian DLA-3682-1 : ncurses - LTS security update]	high
12/3/2023	[AlmaLinux 8 : kpatch-patch (ALSA-2023:7554)]	high
12/3/2023	[AlmaLinux 8 : kernel (ALSA-2023:7549)]	high
12/3/2023	[AlmaLinux 8 : postgresql:13 (ALSA-2023:7581)]	high
12/3/2023	[Fedora 38 : kernel / kernel-headers / kernel-tools (2023-15deb2e32a)]	high
12/3/2023	[Fedora 39 : kernel / kernel-headers / kernel-tools (2023-a7b89262c6)]	high
12/2/2023	[SUSE SLES15 Security Update : ImageMagick (SUSE-SU-2023:4634-1)]	high
12/2/2023	[FreeBSD : varnish – HTTP/2 Rapid Reset Attack (f25a34b1-910d-11ee-a1a2-641c67a117d8)]	high
12/2/2023	[Oracle Linux 8 : kernel (ELSA-2023-7549)]	high
12/2/2023	[openSUSE 15 Security Update : optipng (openSUSE-SU-2023:0388-1)]	high
12/1/2023	[WS_FTP Server Remote Code Execution]	high
12/1/2023	[XML Injection]	high
12/1/2023	[FreeBSD : Gitlab – Vulnerabilities (3b14b2b4-9014-11ee-98b3-001b217b3468)]	high
12/1/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : sqlite3 (SUSE-SU-2023:4619-1)]	high
12/1/2023	[openSUSE 15 Security Update : opera (openSUSE-SU-2023:0385-1)]	high
12/1/2023	[openSUSE 15 Security Update : opera (openSUSE-SU-2023:0386-1)]	high
12/1/2023	[Oracle Linux 8 : postgresql:13 (ELSA-2023-7581)]	high
12/1/2023	[SolarWinds Platform 2023.3.x < 2023.3.1 Multiple Vulnerabilities]	high

Datum	Schwachstelle	Bewertung
12/1/2023	[Debian DSA-5570-1 : nghttp2 - security update]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“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
—
” “Mon, 04 Dec 2023
WordPress Phlox-Pro Theme 5.14.0 Cross Site Scripting
WordPress Phlox-Pro theme version 5.14.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Mon, 04 Dec 2023
BoidCMS 2.0.1 Cross Site Scripting
BoidCMS version 2.0.1 suffers from multiple persistent cross site scripting vulnerabilities.
- Link
—
” “Mon, 04 Dec 2023
GaatiTrack Courier Management System 1.0 SQL Injection
GaatiTrack Courier Management System version 1.0 suffers from a remote SQL 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

Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.