



Ausgabe: 20231213

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

Sicherheitsupdate Apache Struts: Uploadfunktion kann Schadcode passieren lassen

Eine kritische Schwachstelle bedroht das Open-Source-Framework Apache Struts.

- [Link](#)

WordPress Elementor: Halbgarer Sicherheitspatch gefährdete Millionen Websites

Es gibt wichtige Sicherheitsupdates für die WordPress-Plug-ins Backup Migration und Elementor.

- [Link](#)

Patchday: 15 Sicherheitswarnungen von SAP

Am Dezember-Patchday hat SAP 15 neue Sicherheitsmitteilungen herausgegeben. Sie thematisieren teils kritische Lücken.

- [Link](#)

Bluetooth-Lücke: Tastenanschläge in Android, Linux, iOS und macOS einschleusbar

Eine Sicherheitslücke in Bluetooth-Stacks erlaubt Angreifern, Tastenanschläge einzuschmuggeln. Unter Android, iOS, Linux und macOS.

- [Link](#)

Sicherheitslücken: Angreifer können Schadcode auf Qnap NAS schieben

Netzwerkspeicher von Qnap sind verwundbar. In aktuellen Versionen haben die Entwickler Sicherheitsprobleme gelöst.

- [Link](#)

Sicherheitsupdate: WordPress unter bestimmten Bedingungen angreifbar

In der aktuellen WordPress-Version haben die Entwickler eine Sicherheitslücke geschlossen.

- [Link](#)

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](#)

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)

Tue, 12 Dec 2023

[*UPDATE*] [*hoch*] *Siemens SICAM: Mehrere Schwachstellen*

Ein Angreifer kann mehrere Schwachstellen in Siemens SICAM ausnutzen, um Sicherheitsvorkehrungen zu umgehen und Code auszuführen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] Squid: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] Unify OpenScape Desk Phone: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Unify OpenScape Desk Phone ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder seine Privilegien zu erweitern.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] SAP Software: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen um seine Privilegien zu erhöhen, Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Daten zu manipulieren und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] Unify OpenScape Produkte: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Unify OpenScape Produkten ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] Apple Safari: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apple Safari ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] LibreOffice: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Tue, 12 Dec 2023

[NEU] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] binutils: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonym Angreifer kann eine Schwachstelle in binutils ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] Internet Systems Consortium BIND: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Internet Systems Consortium BIND ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] binutils: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in binutils ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder sonstige Auswirkungen zu verursachen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] D-LINK DIR-X3260 Router: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen im D-LINK Router ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

Tue, 12 Dec 2023

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

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

- [Link](#)

Tue, 12 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](#)

Tue, 12 Dec 2023

[UPDATE] [hoch] Intel Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Intel Prozessoren ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern oder Informationen offenzulegen.

- [Link](#)

Mon, 11 Dec 2023

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/12/2023	[RHEL 9 : kpatch-patch (RHSA-2023:7734)]	critical
12/12/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Netatalk vulnerability (USN-6552-1)]	critical
12/12/2023	[Google Chrome < 120.0.6099.109 Multiple Vulnerabilities]	critical
12/12/2023	[RHEL 9 : fence-agents (RHSA-2023:7753)]	critical
12/12/2023	[Ubuntu 18.04 ESM / 20.04 ESM / 22.04 ESM : PostfixAdmin vulnerabilities (USN-6550-1)]	high
12/12/2023	[Ubuntu 23.04 : Linux kernel vulnerabilities (USN-6534-2)]	high
12/12/2023	[RHEL 8 : tracker-miners (RHSA-2023:7739)]	high
12/12/2023	[RHEL 8 : tracker-miners (RHSA-2023:7733)]	high
12/12/2023	[RHEL 8 : tracker-miners (RHSA-2023:7731)]	high
12/12/2023	[RHEL 8 : tracker-miners (RHSA-2023:7732)]	high
12/12/2023	[Adobe Illustrator < 27.9.1 / 28.0 < 28.1 Multiple Arbitrary code execution (APSB23-68)]	high
12/12/2023	[Adobe Illustrator < 27.9.1 / 28.0 < 28.1 Multiple Arbitrary code execution (APSB23-68) (macOS)]	high
12/12/2023	[Ubuntu 20.04 ESM : Pydantic vulnerability (USN-6553-1)]	high
12/12/2023	[Adobe After Effects < 23.6.2 / 24.0.0 < 24.1.0 Multiple Vulnerabilities (APSB23-75)]	high
12/12/2023	[Adobe After Effects < 23.6.2 / 24.0.0 < 24.1.0 Multiple Vulnerabilities (APSB23-75) (macOS)]	high
12/12/2023	[KB5033427: Windows Server 2008 Security Update (December 2023)]	high
12/12/2023	[KB5033118: Windows 2022 / Azure Stack HCI 22H2 Security Update (December 2023)]	high
12/12/2023	[KB5033369: Windows 11 version 21H2 Security Update (December 2023)]	high
12/12/2023	[KB5033383: Windows 11 version 22H2 Security Update (December 2023)]	high
12/12/2023	[KB5033424: Windows Server 2008 R2 Security Update (December 2023)]	high
12/12/2023	[KB5033420: Windows Server 2012 R2 Security Update (December 2023)]	high
12/12/2023	[Security Updates for Azure Connected Machine Agent (December 2023)]	high
12/12/2023	[KB5033379: Windows 10 LTS 1507 Security Update (December 2023)]	high
12/12/2023	[Security Updates for Microsoft Dynamics 365 (on-premises) (December 2023)]	high
12/12/2023	[KB5033372: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (December 2023)]	high
12/12/2023	[KB5033429: Windows Server 2012 Security Update (December 2023)]	high
12/12/2023	[KB5033371: Windows 10 version 1809 / Windows Server 2019 Security Update (December 2023)]	high
12/12/2023	[KB5033375: Windows 11 version 22H2 Security Update (December 2023)]	high
12/12/2023	[KB5033373: Windows 10 Version 1607 and Windows Server 2016 Security Update (December 2023)]	high
12/12/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6548-2)]	high

Datum	Schwachstelle	Bewertung
12/12/2023	[Fedora 38 : libcmis / libreoffice (2023-0d971cd6aa)]	high
12/12/2023	[Fedora 38 : java-17-openjdk (2023-433474a567)]	high
12/12/2023	[RHEL 9 : runc (RHSA-2023:7763)]	high
12/12/2023	[RHEL 9 : tracker-miners (RHSA-2023:7744)]	high
12/12/2023	[RHEL 9 : pixman (RHSA-2023:7754)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Tue, 12 Dec 2023

Splunk XSLT Upload Remote Code Execution

This Metasploit module exploits a remote code execution vulnerability in Splunk Enterprise. The affected versions include 9.0.x before 9.0.7 and 9.1.x before 9.1.2. The exploitation process leverages a weakness in the XSLT transformation functionality of Splunk. Successful exploitation requires valid credentials, typically admin:changeme by default. The exploit involves uploading a malicious XSLT file to the target system. This file, when processed by the vulnerable Splunk server, leads to the execution of arbitrary code. The module then utilizes the runshellsript capability in Splunk to execute the payload, which can be tailored to establish a reverse shell. This provides the attacker with remote control over the compromised Splunk instance. The module is designed to work seamlessly, ensuring successful exploitation under the right conditions.

- [Link](#)

” “Tue, 12 Dec 2023

WordPress Backup Migration 1.3.7 Remote Code Execution

WordPress Backup Migration plugin versions 1.3.7 and below suffer from a remote code execution vulnerability.

- [Link](#)

” “Mon, 11 Dec 2023

WordPress Contact Form To Any API 1.1.6 Cross Site Request Forgery

WordPress Contact Form to Any API plugin versions 1.1.6 and below suffer from a cross site request forgery vulnerability.

- [Link](#)

” “Mon, 11 Dec 2023

WordPress Bravo Translate 1.2 SQL Injection

WordPress Bravo Translate plugin versions 1.2 and below suffer from a remote SQL injection vulnerability.

- [Link](#)

” “Mon, 11 Dec 2023

WordPress TextMe SMS 1.9.0 Cross Site Request Forgery

WordPress TextMe SMS plugin versions 1.9.0 and below suffer from a cross site request forgery vulnerability.

- [Link](#)

” “Sat, 09 Dec 2023

libcue 2.2.1 Out-Of-Bounds Access

libcue provides an API for parsing and extracting data from CUE sheets. Versions 2.2.1 and prior are vulnerable to out-of-bounds array access. A user of the GNOME desktop environment can be exploited by downloading a cue sheet from a malicious webpage. Because the file is saved to ~/Downloads, it is then automatically scanned by tracker-miners. And because it has a .cue filename extension, tracker-miners use libcue to parse the file. The file exploits the vulnerability in libcue to gain code execution. This issue is patched in version 2.3.0. This particular archive holds three proof of concept exploits.

- [Link](#)

” “Fri, 08 Dec 2023

Microsoft Defender Anti-Malware PowerShell API Arbitrary Code Execution

Microsoft Defender API and PowerShell APIs suffer from an arbitrary code execution due to a flaw in powershell not handling user provided input that contains a semicolon.

- [Link](#)

” “Fri, 08 Dec 2023

ISPConfig 3.2.11 PHP Code Injection

ISPConfig versions 4.2.11 and below suffer from a PHP code injection vulnerability in language_edit.php.

- [Link](#)

” “Fri, 08 Dec 2023

osCommerce 4 SQL Injection

osCommerce version 4 suffers from a remote SQL injection vulnerability.

- [Link](#)

” “Fri, 08 Dec 2023

Kopage Website Builder 4.4.15 Shell Upload

Kopage Website Builder version 4.4.15 appears to suffer from a remote shell upload vulnerability.

- [Link](#)

” “Fri, 08 Dec 2023

Windows Kernel Information Disclosure

The Microsoft Windows Kernel has a time-of-check / time-of-use issue in verifying layered key security which may lead to information disclosure from privileged registry keys.

- [Link](#)

” “Fri, 08 Dec 2023

Arm Mali CSF Overflow / Use-After-Free

Arm Mali CSF has a refcount overflow bugfix in r43p0 that was misclassified as a memory leak fix.

- [Link](#)

” “Thu, 07 Dec 2023

ConQuest Dicom Server 1.5.0d Remote Command Execution

Conquest Dicom Server version 1.5.0d pre-authentication remote command execution exploit.

- [Link](#)

” “Thu, 07 Dec 2023

Docker cgroups Container Escape

This Metasploit exploit module takes advantage of a Docker image which has either the privileged flag, or SYS_ADMIN Linux capability. If the host kernel is vulnerable, its possible to escape the Docker image and achieve root on the host operating system. A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.

- [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](#)

”

0-Days der letzten 5 Tage

“Tue, 12 Dec 2023

ZDI-23-1766: Extreme Networks AP410C ah_webui Missing Authentication for Critical Function Remote Code Execution Vulnerability

- [Link](#)

” “Tue, 12 Dec 2023

ZDI-23-1765: Extreme Networks HiveOS ah_auth Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

” “Tue, 12 Dec 2023

ZDI-23-1764: Check Point ZoneAlarm Extreme Security Link Following Local Privilege Escalation Vulnerability

- [Link](#)

”

Die Hacks der Woche

mit Martin Haunschmid

Ihr habt WAS in eure Züge programmiert!?



[Zum Youtube Video](#)

Cyberangriffe: (Dez)

Datum	Opfer	Land	Information
2023-12-12	District de March	[CHE]	Link
2023-12-08	Province des îles Loyauté	[NCL]	Link
2023-12-08	WestPole	[ITA]	Link
2023-12-08	Coaxis	[FRA]	Link
2023-12-07	Aqualectra	[CUW]	Link
2023-12-07	Université de Wollongong	[AUS]	Link
2023-12-07	Prefeitura de Poços de Caldas	[BRA]	Link
2023-12-07	Hinsdale School District	[USA]	Link
2023-12-06	Nissan Oceania	[AUS]	Link
2023-12-06	Gouvernement du Yucatan	[MEX]	Link
2023-12-06	Université de Sherbrooke	[CAN]	Link
2023-12-06	Glendale Unified School District	[USA]	Link
2023-12-05	Dameron Hospital	[USA]	Link
2023-12-05	Gräbener Maschinentchnik	[DEU]	Link
2023-12-04	Caribbean Community (Caricom) Secretariat	[GUY]	Link
2023-12-01	Communauté de communes du Pays du Neubourg	[FRA]	Link

Ransomware-Erpressungen: (Dez)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-12	[King Aerospace, Inc.]	incransom	Link
2023-12-12	[GlobalSpec]	play	Link
2023-12-12	[dena.de]	lockbit3	Link
2023-12-12	[woodruffenterprises.com]	threeam	Link
2023-12-12	[shareharris.com]	threeam	Link
2023-12-12	[SmartWave Technologies]	akira	Link
2023-12-12	[Mitrani Caballero Ojam & Ruiz Moreno - Abogados]	akira	Link
2023-12-12	[The Teaching Company, LLC]	akira	Link
2023-12-12	[Memorial Sloan Kettering Cancer Center]	meow	Link
2023-12-12	[petrotec.com.qa]	lockbit3	Link
2023-12-12	[tradewindscorp-insbrok.com]	lockbit3	Link
2023-12-12	[airtechthelong.com.vn]	lockbit3	Link
2023-12-12	[kitahirosima.jp]	lockbit3	Link
2023-12-12	[Grupo Jose Alves]	rhysida	Link
2023-12-12	[Insomniac Games]	rhysida	Link
2023-12-11	[phillipsglobal.us]	lockbit3	Link
2023-12-11	[greenbriersportingclub.com]	lockbit3	Link
2023-12-11	[ipp-sa.com]	lockbit3	Link
2023-12-11	[r-ab.de]	lockbit3	Link
2023-12-11	[Azienda USL di Modena]	hunters	Link
2023-12-11	[igt.nl]	lockbit3	Link
2023-12-01	[Bayer Heritage Federal Credit Union]	lorenz	Link
2023-12-11	[MSD Information technology]	akira	Link
2023-12-11	[Goiasa]	akira	Link
2023-12-11	[Hinsdale School District]	medusa	Link
2023-12-11	[Independent Recovery Resources, Inc.]	bianlian	Link
2023-12-11	[Studio MF]	akira	Link
2023-12-11	[zailaboratory.com]	lockbit3	Link
2023-12-11	[ISC Consulting Engineers]	cactus	Link
2023-12-11	[The Glendale Unified School District]	medusa	Link
2023-12-10	[pronatindustries.com]	lockbit3	Link
2023-12-10	[policia.gob.pe]	lockbit3	Link
2023-12-10	[Holding Slovenske elektrarne]	rhysida	Link
2023-12-10	[Hse]	rhysida	Link
2023-12-09	[Qatar Racing and Equestrian Club]	rhysida	Link
2023-12-09	[Graphic Solutions Group Inc (US)]	daixin	Link
2023-12-09	[OpTransRights - 2]	siegedsec	Link
2023-12-09	[Telerad]	siegedsec	Link
2023-12-09	[Technical University of Mombasa]	siegedsec	Link
2023-12-09	[National Office for centralized procurement]	siegedsec	Link
2023-12-09	[Portland Government & United states government]	siegedsec	Link
2023-12-09	[Staples]	siegedsec	Link
2023-12-09	[Deqing County]	siegedsec	Link
2023-12-09	[Colombian National Registry]	siegedsec	Link
2023-12-09	[HMW - Press Release]	monti	Link
2023-12-08	[livanova.com]	lockbit3	Link
2023-12-04	[Jerry Pate Energy (hack from Saltmarsh Financial Advisors)]	snatch	Link
2023-12-08	[GOLFZON]	blacksuit	Link
2023-12-08	[aw-lawyers.com]	lockbit3	Link
2023-12-08	[midlandindustries.com]	lockbit3	Link
2023-12-08	[Travian Games]	rhysida	Link
2023-12-08	[Teman]	rhysida	Link
2023-12-07	[California Innovations]	play	Link
2023-12-07	[SMRT]	play	Link
2023-12-07	[Intrepid Sea, Air & Space Museum]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-12-07	[Postworks]	play	Link
2023-12-07	[PLS Logistics]	play	Link
2023-12-07	[Ridge Vineyards]	play	Link
2023-12-07	[AJO]	play	Link
2023-12-07	[PHIBRO GMBH]	play	Link
2023-12-07	[denave.com]	lockbit3	Link
2023-12-07	[Precision Technologies Group Ltd]	incransom	Link
2023-12-07	[Silvent North America]	play	Link
2023-12-07	[GreenWaste Recovery]	play	Link
2023-12-07	[Burton Wire & Cable]	play	Link
2023-12-07	[Capespan]	play	Link
2023-12-07	[Becker Furniture World]	play	Link
2023-12-07	[Payne Hicks Beach]	play	Link
2023-12-07	[Vitro Plus]	play	Link
2023-12-07	[GVM]	play	Link
2023-12-07	[Planbox]	play	Link
2023-12-07	[AG Consulting Engineering]	play	Link
2023-12-07	[Greater Richmond Transit]	play	Link
2023-12-07	[Kuriyama of America]	play	Link
2023-12-07	[bluewaterstt.com]	lockbit3	Link
2023-12-07	[omegapainclinic.com]	lockbit3	Link
2023-12-07	[AMCO Proteins]	bianlian	Link
2023-12-07	[SML Group]	bianlian	Link
2023-12-07	[stormtech]	metaencryptor	Link
2023-12-07	[Garda]	metaencryptor	Link
2023-12-07	[Tri-city Medical Center]	incransom	Link
2023-12-07	[Tasteful Selections]	akira	Link
2023-12-07	[Ware Manufacturing]	qilin	Link
2023-12-07	[Neurology Center of Nevada]	qilin	Link
2023-12-07	[CIE Automotive]	cactus	Link
2023-12-07	[National Nail Corp]	cactus	Link
2023-12-07	[citizenswv.com]	lockbit3	Link
2023-12-07	[directradiology.com]	lockbit3	Link
2023-12-07	[signiflow.com]	lockbit3	Link
2023-12-07	[bpce.com]	lockbit3	Link
2023-12-07	[hopto.com]	lockbit3	Link
2023-12-07	[usherbrooke.ca]	lockbit3	Link
2023-12-07	[Visan]	8base	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[hnnscsb.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.