



Ausgabe: 20231204

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: 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 Plattform 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](#)

Synology schließt Pwn2Own-Lücke in Router-Manager-Firmware

Im Betriebssystem für Synology-Router haben IT-Forscher beim Pwn2Own-Wettbewerb Sicherheitslücken aufgedeckt. Ein Update schließt sie.

- [Link](#)

Sicherheitsupdates: Foxit PDF unter macOS und Windows verwundbar

Die Entwickler haben in aktuellen Versionen von Foxit PDF Reader und PDF Editor 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)

Fri, 01 Dec 2023

[UPDATE] [hoch] *SHA-3 Implementierungen: Schwachstelle ermöglicht Codeausführung*

Ein entfernter, anonymen 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 anonymen 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, anonymen 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

[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](#)

Fri, 01 Dec 2023

[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymen 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](#)

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](#)

Fri, 01 Dec 2023

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] Perl: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Perl ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Thu, 30 Nov 2023

[NEU] [hoch] Tenable Security Nessus Network Monitor: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Tenable Security Nessus Network Monitor ausnutzen, um vertrauliche Informationen offenzulegen, beliebigen Code auszuführen oder Dateien zu manipulieren.

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] PostgreSQL JDBC Treiber: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle im PostgreSQL JDBC Treiber ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Thu, 30 Nov 2023

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

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

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] Apache Struts: Schwachstelle ermöglicht Denial of Service

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

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonym Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Thu, 30 Nov 2023

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

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

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/1/2023	[OwnCloud graphapi 0.2.x < 0.2.1 / 0.3.x < 0.3.1 Sensitive Informations Disclosure]	critical
12/1/2023	[Apple iOS < 17.1.2 Multiple Vulnerabilities (HT214031)]	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
11/30/2023	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6496-2)]	critical
11/30/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6495-2)]	critical
11/30/2023	[Ubuntu 16.04 ESM / 18.04 ESM : Linux kernel vulnerabilities (USN-6494-2)]	critical
11/30/2023	[Ubuntu 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6502-4)]	critical
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 : electron25 – multiple vulnerabilities (302fc846-860f-482e-a8f6-ee9f254dfacf)]	high
12/1/2023	[FreeBSD : electron26 – multiple vulnerabilities (7e1a508f-7167-47b0-b9fc-95f541933a86)]	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	[openSUSE 15 Security Update : chromium (openSUSE-SU-2023:0387-1)]	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
12/1/2023	[Debian DSA-5569-1 : chromium - security update]	high
12/1/2023	[Debian DSA-5570-1 : nghttp2 - security update]	high
11/30/2023	[Debian DLA-3677-1 : gimp-dds - LTS security update]	high
11/30/2023	[Debian DLA-3676-1 : libde265 - LTS security update]	high
11/30/2023	[Fedora 39 : java-17-openjdk (2023-b6612f3819)]	high
11/30/2023	[Fedora 39 : golang-github-google-dap (2023-fa2ec3d3e0)]	high

Datum	Schwachstelle	Bewertung
11/30/2023	[Fedora 38 : golang-github-google-dap (2023-548163deb1)]	high
11/30/2023	[Fedora 37 : golang-github-google-dap (2023-c858d2c53b)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits der letzten 5 Tage

“Fri, 01 Dec 2023

Packet Storm New Exploits For November, 2023

This archive contains all of the 49 exploits added to Packet Storm in November, 2023.

- [Link](#)

” “Fri, 01 Dec 2023

Kopage Website Builder 4.4.15 Cross Site Scripting

Kopage Website Builder version 4.4.15 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

” “Fri, 01 Dec 2023

WBCE CMS 1.6.1 Shell Upload

WBCE CMS version 1.6.1 suffers from a remote shell upload vulnerability.

- [Link](#)

” “Thu, 30 Nov 2023

CE Phoenix 1.0.8.20 Remote Code Execution

CE Phoenix version 1.0.8.20 remote code execution exploit written in Python.

- [Link](#)

” “Thu, 30 Nov 2023

Online Student Clearance System 1.0 Shell Upload

Online Student Clearance System versions 1.0 and below suffer from a remote shell upload vulnerability.

- [Link](#)

” “Wed, 29 Nov 2023

WordPress Royal Elementor Addons And Templates Remote Shell Upload

WordPress Royal Elementor Addons and Templates plugin versions prior to 1.3.79 suffer from a remote shell upload vulnerability.

- [Link](#)

” “Tue, 28 Nov 2023

Fortra Digital Guardian Agent Uninstaller Cross Site Scripting / UninstallKey Cached

The uninstaller in Fortra Digital Guardian Agent versions prior to 7.9.4 suffers from a cross site scripting vulnerability. Additionally, the Agent Uninstaller handles sensitive data insecurely and caches the Uninstall key in memory. This key can be used to stop or uninstall the application. This allows a locally authenticated attacker with administrative privileges to disable the application temporarily or even remove the application from the system completely.

- [Link](#)

” “Tue, 28 Nov 2023

etcd-browser 87ae63d75260 Directory Traversal

etcd-browser version 87ae63d75260 suffers from a directory traversal vulnerability.

- [Link](#)

” “Tue, 28 Nov 2023

Loytec L-INX Automation Servers Information Disclosure / Cleartext Secrets

Loytec LINX-151 with firmware version 7.2.4 and LINX-212 with firmware version 6.2.4 suffer from file disclosure vulnerabilities that leak secrets as well as issues with storing secrets in the clear.

- [Link](#)

” “Tue, 28 Nov 2023

Loytec LINX Configurator 7.4.10 Insecure Transit / Cleartext Secrets

Loytec LINX Configurator version 7.4.10 suffers from insecure transit and cleartext hardcoded secret vulnerabilities.

- [Link](#)

” “Tue, 28 Nov 2023

WebRTC PacketRouter Dangling Entry

A dangling pointer vulnerability is present in WebRTC’s PacketRouter due to an SDP SIM group SSRC from one track (e.g., video) colliding with an existing SSRC from a different track (e.g., audio). This inconsistency between the `send_modules_map` and the `send_modules_list` can lead to a use after free.

- [Link](#)

” “Tue, 28 Nov 2023

m-privacy TightGate-Pro Code Execution / Insecure Permissions

m-privacy TightGate-Pro suffers from code execution, insecure permissions, deletion mitigation, and outdated server vulnerabilities.

- [Link](#)

” “Tue, 28 Nov 2023

SmartNode SN200 3.21.2-23021 OS Command Injection

SmartNode SN200 versions 3.21.2-23021 and below suffer from a remote command execution vulnerability.

- [Link](#)

” “Mon, 27 Nov 2023

TitanNit Web Control 2.01 / Atemio 7600 Root Remote Command Execution

The Atemio AM 520 HD Full HD satellite receiver has a vulnerability that enables an unauthorized attacker to execute system commands with elevated privileges. This exploit is facilitated through the use of the `getcommand` query within the application, allowing the attacker to gain root access. Firmware versions 2.01 and below are affected.

- [Link](#)

” “Mon, 27 Nov 2023

osCommerce 4 Cross Site Scripting

osCommerce version 4 suffers from a cross site scripting vulnerability.

- [Link](#)

” “Mon, 27 Nov 2023

PopojiCMS 2.0.1 Remote Command Execution

PopojiCMS version 2.0.1 suffers from a remote command execution vulnerability.

- [Link](#)

” “Mon, 27 Nov 2023

CSZ CMS 1.3.0 Remote Command Execution

CSZ CMS version 1.3.0 suffers from a remote command execution vulnerability. Exploit written in Python.

- [Link](#)

” “Mon, 27 Nov 2023

CE Phoenix 1.0.8.20 Remote Command Execution

CE Phoenix version 1.0.8.20 suffers from an authenticated remote command execution vulnerability.

- [Link](#)

” “Sat, 25 Nov 2023

CE Phoenix 1.0.8.20 Cross Site Scripting

CE Phoenix version 1.0.8.20 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

” “Sat, 25 Nov 2023

PyroCMS 3.0.1 Cross Site Scripting

PyroCMS version 3.0.1 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

” “Sat, 25 Nov 2023

CSZ CMS 1.3.0 Shell Upload

CSZ CMS version 1.3.0 suffers from a remote shell upload vulnerability.

- [Link](#)

” “Wed, 22 Nov 2023

WordPress UserPro 5.1.x Password Reset / Authentication Bypass / Escalation

WordPress UserPro plugin versions 5.1.1 and below suffer from an insecure password reset mechanism, information disclosure, and authentication bypass vulnerabilities. Versions 5.1.4 and below suffer from privilege escalation and shortcode execution vulnerabilities.

- [Link](#)

” “Mon, 20 Nov 2023

Magento 2.4.6 XSLT Server Side Injection

Magento version 2.4.6 XSLT server-side injection proof of concept exploit.

- [Link](#)

” “Mon, 20 Nov 2023

PHPJabbers Availability Booking Calendar 5.0 Cross Site Scripting

PHPJabbers Availability Booking Calendar version 5.0 suffers from multiple cross site scripting vulnerabilities.

- [Link](#)

” “Mon, 20 Nov 2023

PHPJabbers Availability Booking Calendar 5.0 CSV Injection

PHPJabbers Availability Booking Calendar version 5.0 suffers from a CSV injection vulnerability.

- [Link](#)

”

0-Days der letzten 5 Tage

“Thu, 30 Nov 2023

ZDI-23-1756: Delta Electronics InfraSuite Device Master PlayWaveFile Directory Traversal Information Disclosure Vulnerability

- [Link](#)

” “Thu, 30 Nov 2023

ZDI-23-1755: Delta Electronics InfraSuite Device Master RunScript Exposed Dangerous Method Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 30 Nov 2023

ZDI-23-1754: Delta Electronics InfraSuite Device Master Device-DataCollect Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 30 Nov 2023

ZDI-23-1753: Delta Electronics InfraSuite Device Master Device-Gateway Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

” “Thu, 30 Nov 2023

ZDI-23-1752: Delta Electronics InfraSuite Device Master UploadMedia Directory Traversal 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-Gruppe	Webseite
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.