
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240112



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	6
3.3 Sicherheitslücken Meldungen von Tenable	10
4 Aktiv ausgenutzte Sicherheitslücken	11
4.1 Exploits der letzten 5 Tage	11
4.2 0-Days der letzten 5 Tage	15
5 Die Hacks der Woche	22
5.0.1 Diese Idee hätte ich WIRKLICH gerne selbst gehabt (über 100k Bug Bounty) . .	22
6 Cyberangriffe: (Jan)	23
7 Ransomware-Erpressungen: (Jan)	23
8 Quellen	25
8.1 Quellenverzeichnis	25
9 Impressum	27

1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

Splunk, cacti, checkmk: Sicherheitslücken in Monitoring-Software

In drei beliebten Monitoring-Produkten gibt es Sicherheitsprobleme. Admins sollten sich um Updates kümmern.

- [Link](#)

—

Juniper Networks bessert zahlreiche Schwachstellen aus

Juniper Networks hat 27 Sicherheitsmitteilungen veröffentlicht. Sie betreffen Junos OS, Junos OS Evolved und diverse Hardware.

- [Link](#)

—

Sicherheitspatch: IBM Security Verify für Root-Attacken anfällig

Die Entwickler haben in IBMs Zugriffsmanagementlösung Security Verify mehrere Sicherheitslücken geschlossen.

- [Link](#)

—

Zoho ManageEngine: Kritische Sicherheitslücke in ADSelfService Plus

In Zoho ManageEngine ADSelfService Plus klafft eine kritische Sicherheitslücke. Angreifer können dadurch Schadcode einschleusen.

- [Link](#)

—

Sicherheitsupdates für Dell- und Lenovo-BIOS

Dell stellt aktualisierte BIOS-Versionen für einige Geräte bereit. AMI schließt mehrere Sicherheitslücken, Lenovo reicht die Korrekturen durch.

- [Link](#)

—

Sicherheitspatch: API-Fehler in Cisco Unity Connection macht Angreifer zum Root

Verschiedene Netzwerkprodukte von Cisco sind verwundbar. Eine Lücke gilt als kritisch.

- [Link](#)

—

Zerodays bei Ivanti aktiv genutzt: Connect Secure und Policy Secure sinds nicht

Zwei Zero-Days in Ivanti-Produkten machen es "trivial für Angreifer", Befehle auszuführen und sich im Firmennetz einzunisten. Ivanti hat bedingt gute Tipps.

- [Link](#)

—

Webkonferenzen: Zoom-Sicherheitslücken ermöglichen Rechteausweitung

Zoom verteilt aktualisierte Videokonferenz-Software. Sie schließt eine Sicherheitslücke, durch die Angreifer ihre Rechte ausweiten können.

- [Link](#)

—

Fortinet: Sicherheitsupdate gegen Rechteverwaltungsfehler in FortiOS und -Proxy

Fortinet warnt vor einem Fehler in der Rechteverwaltung von FortiOS und FortiProxy in HA Clustern. Böartige Akteure können ihre Rechte ausweiten.

- [Link](#)

—

Patchday Adobe: Mehrere Schwachstellen in Substance 3D Stager geschlossen

Adobes Anwendung zum Erstellen von 3D-Szenen Substance 3D Stager ist angreifbar. Eine fehlerbereinigte Version steht zum Download bereit.

- [Link](#)

—

3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-5360	0.967230000	0.995820000	Link
CVE-2023-4966	0.925220000	0.987920000	Link
CVE-2023-46747	0.965530000	0.995220000	Link
CVE-2023-46604	0.971470000	0.997580000	Link
CVE-2023-42793	0.972830000	0.998360000	Link
CVE-2023-38035	0.971630000	0.997650000	Link
CVE-2023-35078	0.948640000	0.991100000	Link
CVE-2023-34634	0.906880000	0.985870000	Link
CVE-2023-33246	0.971220000	0.997470000	Link
CVE-2023-32315	0.964530000	0.994800000	Link
CVE-2023-30625	0.937080000	0.989370000	Link
CVE-2023-30013	0.944370000	0.990360000	Link
CVE-2023-29300	0.933050000	0.988890000	Link
CVE-2023-28771	0.923800000	0.987750000	Link
CVE-2023-27524	0.962250000	0.994060000	Link
CVE-2023-27372	0.970430000	0.997010000	Link
CVE-2023-27350	0.972430000	0.998110000	Link
CVE-2023-26469	0.938510000	0.989520000	Link
CVE-2023-26360	0.942270000	0.989990000	Link
CVE-2023-26035	0.968020000	0.996110000	Link
CVE-2023-25717	0.954350000	0.992230000	Link
CVE-2023-25194	0.910840000	0.986270000	Link
CVE-2023-2479	0.958820000	0.993240000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.968700000	0.996360000	Link
CVE-2023-23752	0.961870000	0.993970000	Link
CVE-2023-22518	0.965250000	0.995070000	Link
CVE-2023-22515	0.957080000	0.992840000	Link
CVE-2023-21839	0.962040000	0.994030000	Link
CVE-2023-21823	0.940060000	0.989710000	Link
CVE-2023-21554	0.961220000	0.993770000	Link
CVE-2023-20887	0.961530000	0.993840000	Link
CVE-2023-1671	0.953130000	0.991960000	Link
CVE-2023-0669	0.968210000	0.996160000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 11 Jan 2024

[NEU] [hoch] tribe29 checkmk: Mehrere Schwachstellen

Ein authentifizierter Angreifer kann mehrere Schwachstellen in tribe29 checkmk ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 11 Jan 2024

[NEU] [hoch] Juniper Produkte: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer, authentisierter, lokaler oder physischer Angreifer kann mehrere Schwachstellen in Juniper JUNOS, Juniper JUNOS Evolved, Juniper SRX Series, Juniper EX Series, Juniper QFX Series, Juniper ACX Series, Juniper PTX Series und Juniper MX Series ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und seine Berechtigungen zu erweitern.

- [Link](#)

—

Thu, 11 Jan 2024

[NEU] [hoch] Cisco Unity Connection: Schwachstelle ermöglicht Privilegienerweiterung und Codeausführung

Ein entfernter anonymer Angreifer kann eine Schwachstelle in Cisco Unity Connection ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.

- [Link](#)

—

Thu, 11 Jan 2024

[NEU] [UNGEPATCHT] [kritisch] Ivanti Connect Secure: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure und Ivanti Policy Secure ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder um beliebigen Code auszuführen.

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] NCP Secure Enterprise Client: Schwachstelle ermöglicht Privilegieneskalation und Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in NCP Secure Enterprise Client ausnutzen, um seine Privilegien zu erhöhen und zur Ausführung von beliebigem Code.

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in libarchive ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Thu, 11 Jan 2024

[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](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

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

- [Link](#)

—

Thu, 11 Jan 2024

[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, 11 Jan 2024

[UPDATE] [hoch] Verschiedene D-LINK Router und Access Point Modelle: Mehrere Schwachstellen

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in verschiedenen D-LINK Routern und Access Points ausnutzen, um die Netzwerkinfrastruktur anzugreifen, beliebigen Code auszuführen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Thu, 11 Jan 2024

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

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

- [Link](#)

—

Thu, 11 Jan 2024

[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, 11 Jan 2024

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

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

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [kritisch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 11 Jan 2024

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

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

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen oder Dateien zu manipulieren.

- [Link](#)

—

Thu, 11 Jan 2024

[UPDATE] [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](#)

—

Thu, 11 Jan 2024

[UPDATE] [hoch] Zabbix: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder Code auszuführen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/11/2024	[Ubuntu 22.04 LTS / 23.04 / 23.10 : .NET vulnerabilities (USN-6578-1)]	critical
1/11/2024	[GitLab 8.13 < 16.5.6 / 16.6 < 16.6.4 / 16.7 < 16.7.2 (CVE-2023-5356)]	critical
1/11/2024	[GitLab 16.1 < 16.5.6 / 16.6 < 16.6.4 / 16.7 < 16.7.2 (CVE-2023-7028)]	critical
1/10/2024	[Fedora 39 : chromium (2024-01607ac0ae)]	critical
1/11/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Go vulnerabilities (USN-6574-1)]	high
1/11/2024	[SUSE SLED12 / SLES12 Security Update : LibreOffice (SUSE-SU-2024:0075-1)]	high
1/11/2024	[openSUSE 15 Security Update : opera (openSUSE-SU-2024:0016-1)]	high
1/11/2024	[Siemens JT2Go < 14.3.0.6 Multiple Vulnerabilities (SSA-794653)]	high
1/11/2024	[Trellix Agent < 5.8.1 Buffer Overflow Vulnerability (SB10416)]	high
1/11/2024	[Atlassian Jira Service Management Data Center and Server 4.20.x < 4.20.28 / 5.4.x < 5.4.12 / 5.5.x < 5.11.3 / 5.12.0 (JSDSERVER-14873)]	high
1/11/2024	[Fortinet FortiOS Privilege Escalation (FG-IR-23-315)]	high
1/11/2024	[Fortinet FortiProxy Privilege Escalation (FG-IR-23-315)]	high
1/11/2024	[Atlassian JIRA Service Desk < 4.20.28 / 5.4.x < 5.4.12 / 5.5.x < 5.11.3 / 5.12.0 (JSDSERVER-14872)]	high
1/11/2024	[Oracle Linux 8 : pixman (ELSA-2024-0131)]	high
1/11/2024	[Ubuntu 16.04 ESM / 18.04 ESM : Xerces-C++ vulnerability (USN-6579-1)]	high

Datum	Schwachstelle	Bewertung
1/11/2024	[GitLab 15.3 < 16.5.6 / 16.6 < 16.6.4 / 16.7 < 16.7.2 (CVE-2023-4812)]	high
1/11/2024	[Fedora 39 : openssh (2024-7e301327c2)]	high
1/11/2024	[Fedora 38 : tinymce (2024-c9dc0ac419)]	high
1/11/2024	[Oracle Linux 8 : kernel (ELSA-2024-12069)]	high
1/11/2024	[Siemens SCALANCE OpenSSL NULL Pointer Dereference (CVE-2023-0217)]	high
1/11/2024	[Siemens SCALANCE OpenSSL NULL Pointer Dereference (CVE-2023-0401)]	high
1/11/2024	[Siemens SCALANCE OpenSSL NULL Pointer Dereference (CVE-2023-0216)]	high
1/10/2024	[Oracle Linux 8 : python-urllib3 (ELSA-2024-0116)]	high
1/10/2024	[Oracle Linux 8 : python3 (ELSA-2024-0114)]	high
1/10/2024	[Ubuntu 20.04 LTS : Linux kernel (IoT) vulnerabilities (USN-6548-5)]	high
1/10/2024	[Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-6549-5)]	high
1/10/2024	[Ubuntu 22.04 LTS : Linux kernel (OEM) vulnerability (USN-6576-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 11 Jan 2024

WordPress POST SMTP Mailer 2.8.7 Authorization Bypass / Cross Site Scripting

WordPress POST SMTP Mailer plugin versions 2.8.7 and below suffer from authorization bypass and cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

SimpleWebServer 2.2-rc2 Denial Of Service

SimpleWebServer version 2.2-rc2 remote denial of service exploit.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Event Ticketing System 1.0 Missing Rate Limiting

PHPJabbers Event Ticketing System version 1.0 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Meeting Room Booking System 1.0 CSV Injection

PHPJabbers Meeting Room Booking System version 1.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Meeting Room Booking System 1.0 Cross Site Scripting

PHPJabbers Meeting Room Booking System version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Event Ticketing System 1.0 Cross Site Scripting / HTML Injection

PHPJabbers Event Ticketing System version 1.0 suffers from cross site scripting and html injection vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Cinema Booking System 1.0 Missing Rate Limiting

PHPJabbers Cinema Booking System version 1.0 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Cinema Booking System 1.0 CSV Injection

PHPJabbers Cinema Booking System version 1.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Meeting Room Booking System 1.0 Missing Rate Limiting

PHPJabbers Meeting Room Booking System version 1.0 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Cleaning Business Software 1.0 CSV Injection

PHPJabbers Cleaning Business Software version 1.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Cinema Booking System 1.0 Cross Site Scripting

PHPJabbers Cinema Booking System version 1.0 suffers from reflective and persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Cleaning Business Software 1.0 Cross Site Scripting

PHPJabbers Cleaning Business Software version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Cleaning Business Software 1.0 Missing Rate Limiting

PHPJabbers Cleaning Business Software version 1.0 suffers from multiple missing rate limiting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Shared Asset Booking System 1.0 Cross Site Scripting

PHPJabbers Shared Asset Booking System version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Shared Asset Booking System 1.0 CSV Injection

PHPJabbers Shared Asset Booking System version 1.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Shared Asset Booking System 1.0 Missing Rate Limit

PHPJabbers Shared Asset Booking System version 1.0 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Night Club Booking Software 1.0 Missing Rate Limiting

PHPJabbers Night Club Booking Software version 1.0 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Night Club Booking Software 1.0 CSV Injection

PHPJabbers Night Club Booking Software version 1.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Bus Reservation System 1.1 CSV Injection

PHPJabbers Bus Reservation System version 1.1 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Bus Reservation System 1.1 Cross Site Scripting

PHPJabbers Bus Reservation System version 1.1 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Restaurant Booking System 3.0 CSV Injection

PHPJabbers Restaurant Booking System version 3.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Bus Reservation System 1.1 Missing Rate Limiting

PHPJabbers Bus Reservation System version 1.1 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Restaurant Booking System 3.0 Missing Rate Limiting

PHPJabbers Restaurant Booking System version 3.0 suffers from a missing rate limiting vulnerability.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Event Booking Calendar 4.0 Missing Rate Limiting

PHPJabbers Event Booking Calendar version 4.0 suffers from multiple missing rate limiting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Jan 2024

PHPJabbers Car Park Booking System 3.0 CSV Injection

PHPJabbers Car Park Booking System version 3.0 suffers from a CSV injection vulnerability.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 11 Jan 2024

ZDI-24-071: Ivanti Avalanche WLAvalancheService Integer Underflow Denial-of-Service Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-070: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-069: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-068: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-067: Ivanti Avalanche WLAvalancheService Divide By Zero Denial-of-Service Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-066: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-065: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-064: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-063: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-062: Ivanti Avalanche WLAvalancheService Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-061: Ivanti Avalanche WLAvalancheService TV_FC Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-060: Ivanti Avalanche WLAvalancheService TV_NL Null Pointer Dereference Denial-of-Service Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-059: Ivanti Avalanche WLInfoRailService Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-058: Ivanti Avalanche SecureFilter allowPassThrough Authentication Bypass Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-057: Ivanti Avalanche SecureFilter Content-Type Authentication Bypass Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-056: Ivanti Avalanche FileStoreConfig Arbitrary File Upload Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-055: Ivanti Avalanche FileStoreConfig Arbitrary File Upload Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-054: Ivanti Avalanche decode XML External Entity Processing Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-053: Ivanti Avalanche validateAMCWSSConnection Server-Side Request Forgery Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-052: Trend Micro Apex Central modVulnerabilityProtect Server-Side Request Forgery Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-051: Trend Micro Apex Central Cross-Site Scripting Privilege Escalation Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-050: D-Link DIR-X3260 prog.cgi SetUsersSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-049: D-Link DCS-8300LHV2 ONVIF Hardcoded PIN Authentication Bypass Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-048: D-Link DCS-8300LHV2 ONVIF SetHostName Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-047: D-Link DCS-8300LHV2 ONVIF Duration Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-046: D-Link DCS-8300LHV2 RTSP ValidateAuthorizationHeader Username Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-045: D-Link DCS-8300LHV2 ONVIF SetSystemDateAndTime Command Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-044: D-Link DCS-8300LHV2 RTSP ValidateAuthorizationHeader Nonce Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-043: D-Link DIR-X3260 prog.cgi SetAPClientSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-042: D-Link DIR-X3260 prog.cgi SetTriggerPPPoEValidate Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-041: D-Link DIR-X3260 prog.cgi SetDeviceSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-040: D-Link DIR-X3260 prog.cgi SetIPv6PppoeSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-039: D-Link DIR-X3260 prog.cgi SetMyDLinkRegistration Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-038: D-Link DIR-X3260 prog.cgi SetWlanRadioSecurity Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-037: D-Link DIR-X3260 prog.cgi SetWanSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-036: D-Link DIR-X3260 prog.cgi SetSysEmailSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-035: D-Link DIR-X3260 prog.cgi SetQuickVPNSettings PSK Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-034: D-Link DIR-X3260 prog.cgi SetQuickVPNSettings Password Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Thu, 11 Jan 2024

ZDI-24-033: D-Link DIR-X3260 prog.cgi SetDynamicDNSSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-032: Foxit PDF Reader Doc Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-031: Microsoft Windows cldflt Integer Overflow Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-030: Microsoft Office Word FBX File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-029: Trend Micro Apex One Exposed Dangerous Function Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-028: Trend Micro Apex One Security Agent Updater Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-027: Trend Micro Apex One Anti-Spyware Engine Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-026: Trend Micro Apex One Virus Scan Engine Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-025: Trend Micro Apex One Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-024: Trend Micro Apex Central widget WFPProxy Local File Inclusion Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-023: Trend Micro Apex Central Cross-Site Scripting Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-022: Trend Micro Apex Central Cross-Site Scripting Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 10 Jan 2024

ZDI-24-021: Trend Micro Apex Central Cross-Site Scripting Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 09 Jan 2024

ZDI-24-020: Linux Kernel GSM Multiplexing Race Condition Local Privilege Escalation Vulnerability

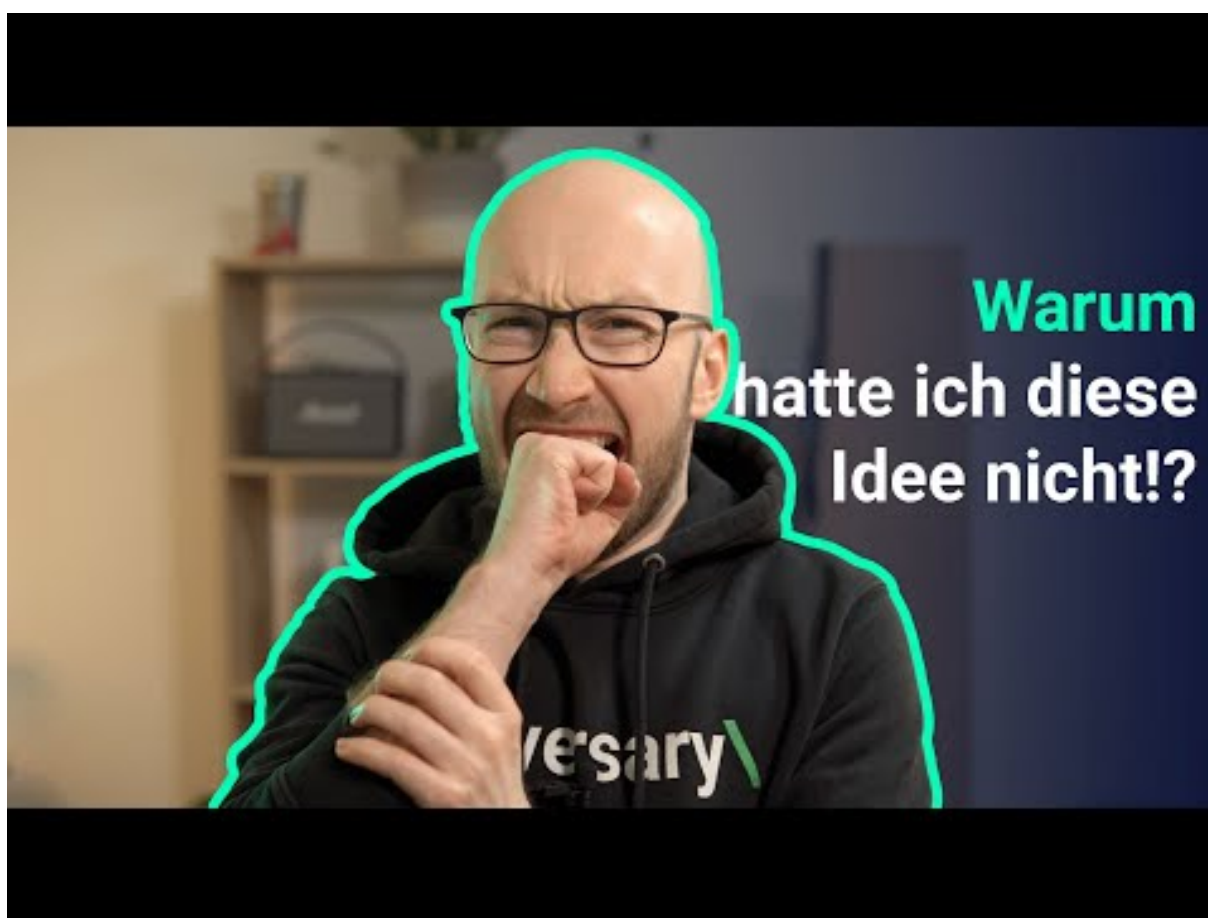
- [Link](#)

—
”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Diese Idee hätte ich WIRKLICH gerne selbst gehabt (über 100k Bug Bounty)



[Zum Youtube Video](#)

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-10	RE&S Holdings	[SGP]	Link
2024-01-10	Lush	[GBR]	Link
2024-01-06	loanDepot	[USA]	Link
2024-01-05	Toronto Zoo	[CAN]	Link
2024-01-05	ODAV AG	[DEU]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-12	[acutis.com]	cactus	Link
2024-01-12	[dtsolutions.net]	cactus	Link
2024-01-12	[intercityinvestments.com]	cactus	Link
2024-01-12	[hi-cone.com]	cactus	Link
2024-01-12	[Alliedwoundcare]	everest	Link
2024-01-12	[Primeimaging]	everest	Link
2024-01-11	[Blackburn College]	akira	Link
2024-01-11	[Vincentz Network]	akira	Link
2024-01-11	[Limburg]	medusa	Link
2024-01-11	[Water For People]	medusa	Link
2024-01-11	[pactchangeslives.com]	lockbit3	Link
2024-01-11	[Triella]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-11	[Ursel Phillips Fellows Hopkinson]	alphv	Link
2024-01-11	[SHIBLEY RIGHTON]	alphv	Link
2024-01-11	[automotionsshade.com]	alphv	Link
2024-01-11	[R Robertson Insurance Brokers]	alphv	Link
2024-01-10	[molnar&partner]	qilin	Link
2024-01-10	[hartalega.com.my]	lockbit3	Link
2024-01-10	[agnesb.eu]	lockbit3	Link
2024-01-10	[twi.co.za]	lockbit3	Link
2024-01-10	[tiautoinvestments.co.za]	lockbit3	Link
2024-01-10	[Group Bogart]	alphv	Link
2024-01-09	[Delco Automation]	blacksuit	Link
2024-01-09	[Viridi]	akira	Link
2024-01-09	[Ito Pallpack Gruppen]	akira	Link
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	Link
2024-01-09	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	Link

8 Quellen

8.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>

- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - packetstormsecurity.com
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

9 Impressum



Herausgeber:

Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail

info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.