Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240814

Inhaltsverzeichnis

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

Patchday: Angreifer können SAP BusinessObjects kompromittieren
Die SAP-Entwickler haben unter anderem kritische Sicherheitslücken in ihrer Unternehmenssoftware geschlossen.
- Link

—

Sicherheitslücken: Netzwerkmonitoringtool Zabbix kann Passwörter leaken
Unter anderen eine kritische Schadcode-Lücke bedroht Zabbix. Dagegen abgesicherte Versionen stehen zum Download bereit.
- Link

—

Root-Sicherheitslücke bedroht Datenbankmanagementsystem PostgreSQL
Die PostgreSQL-Entwickler haben in aktuellen Versionen eine Schwachstelle geschlossen. Angreifer können Schadcode ausführen.
- Link

—

VPN-Clients und Passwortmanager betroffen: Klartextpasswort im Prozessspeicher
Wegen einer Lücke unter anderem in VPN-Clients und Passwortmanagern bleiben vertrauliche Daten auch nach Abmeldung im Prozess-Speicher und sind auslesbar.
- Link

—

CPU-Sicherheitslücke in AMD-Prozessoren ermöglicht Malware-Infektionen
Sicherheitsforscher haben eine als Sinkclose bezeichnete Sicherheitslücke in AMD-CPUs entdeckt und auf der Defcon 32 in Las Vegas präsentiert.
- Link

—

Sicherheitstipps Cisco: Angreifer missbrauchen Smart-Install-Protokoll
Ein Dienst zur Fernkonfiguration für Switches von Cisco und schwache Passwörter spielen Angreifer in die Karten. Doch dagegen können Admins etwas machen.
- Link

—

Attacken auf Android-Kernel, Apache OfBiz und Progress WhatsUp
Auf Sicherheitslücken im Android-Kernel, Apache OfBiz und Progress WhatsUp finden inzwischen Angriffe in freier Wildbahn statt.
- Link

—

Roundcube Webmail: Angreifer können durch kritische Lücke E-Mails kapern

Admins sollten Roundcube aus Sicherheitsgründen auf den aktuellen Stand bringen. Viele Universitäten setzen auf dieses Webmailprodukt.

- Link

—

Cisco: Angreifer können Befehle auf IP-Telefonen ausführen, Update kommt nicht

Für kritische Lücken in Cisco-IP-Telefonen wird es keine Updates geben. Für eine jüngst gemeldete Lücke ist ein Proof-of-Concept-Exploit aufgetaucht.

- Link

—

TeamCity: Fehlerhafte Rechtevergabe ermöglicht Rechteausweitung

Eine Sicherheitslücke in TeamCity ermöglicht Angreifern, ihre Rechte auszuweiten. Ein bereitstehendes Update korrigiert den Fehler.

- 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-2023-7028	0.903160000	0.988670000	Link
CVE-2023-6895	0.922010000	0.990040000	Link
CVE-2023-6553	0.927320000	0.990640000	Link
CVE-2023-5360	0.903980000	0.988730000	Link
CVE-2023-52251	0.944080000	0.992490000	Link
CVE-2023-4966	0.971280000	0.998280000	Link
CVE-2023-49103	0.962110000	0.995570000	Link
CVE-2023-48795	0.964660000	0.996160000	Link
CVE-2023-47246	0.961760000	0.995500000	Link
CVE-2023-46805	0.937250000	0.991670000	Link
CVE-2023-46747	0.972820000	0.998880000	Link
CVE-2023-46604	0.961790000	0.995500000	Link
CVE-2023-4542	0.928310000	0.990740000	Link
CVE-2023-43208	0.966400000	0.996670000	Link
CVE-2023-43177	0.964550000	0.996150000	Link
CVE-2023-42793	0.969020000	0.997440000	Link
CVE-2023-41265	0.911110000	0.989220000	Link
CVE-2023-39143	0.939130000	0.991900000	Link
CVE-2023-38646	0.906610000	0.988890000	Link
CVE-2023-38205	0.947910000	0.993070000	Link
CVE-2023-38203	0.966410000	0.996690000	Link
CVE-2023-38146	0.920720000	0.989880000	Link
CVE-2023-38035	0.974680000	0.999700000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966270000	0.996650000	Link
CVE-2023-3519	0.965340000	0.996420000	Link
CVE-2023-35082	0.966130000	0.996600000	Link
CVE-2023-35078	0.970390000	0.997920000	Link
CVE-2023-34993	0.972640000	0.998790000	Link
CVE-2023-34960	0.928290000	0.990730000	Link
CVE-2023-34634	0.925130000	0.990430000	Link
CVE-2023-34468	0.906650000	0.988900000	Link
CVE-2023-34362	0.971000000	0.998160000	Link
CVE-2023-34039	0.947770000	0.993010000	Link
CVE-2023-3368	0.932420000	0.991210000	Link
CVE-2023-33246	0.972140000	0.998580000	Link
CVE-2023-32315	0.970550000	0.997980000	Link
CVE-2023-30625	0.953800000	0.994090000	Link
CVE-2023-30013	0.962380000	0.995630000	Link
CVE-2023-29300	0.968930000	0.997420000	Link
CVE-2023-29298	0.947600000	0.992990000	Link
CVE-2023-28432	0.906190000	0.988860000	Link
CVE-2023-28343	0.942300000	0.992270000	Link
CVE-2023-28121	0.909500000	0.989080000	Link
CVE-2023-27524	0.970600000	0.998010000	Link
CVE-2023-27372	0.972120000	0.998560000	Link
CVE-2023-27350	0.969720000	0.997710000	Link
CVE-2023-26469	0.956020000	0.994530000	Link
CVE-2023-26360	0.965230000	0.996370000	Link
CVE-2023-26035	0.967360000	0.996950000	Link
CVE-2023-25717	0.954250000	0.994180000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.968820000	0.997390000	Link
CVE-2023-2479	0.963740000	0.995950000	Link
CVE-2023-24489	0.973870000	0.999300000	Link
CVE-2023-23752	0.956380000	0.994580000	Link
CVE-2023-23333	0.958950000	0.994960000	Link
CVE-2023-22527	0.968290000	0.997230000	Link
CVE-2023-22518	0.964890000	0.996200000	Link
CVE-2023-22515	0.973250000	0.999050000	Link
CVE-2023-21839	0.955020000	0.994330000	Link
CVE-2023-21554	0.952830000	0.993910000	Link
CVE-2023-20887	0.970670000	0.998020000	Link
CVE-2023-1671	0.962480000	0.995640000	Link
CVE-2023-0669	0.969440000	0.997590000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 13 Aug 2024

[NEU] [hoch] Zoom Video Communications Rooms: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zoom Video Communications Rooms ausnutzen, um Informationen offenzulegen, seine Rechte zu erweitern oder einen Denial-of-Service-Zustand auszulösen.

- Link

—

Tue, 13 Aug 2024

[NEU] [hoch] SAP Security Patch Day – August 2024

Ein Angreifer kann mehrere Schwachstellen in der SAP-Software ausnutzen, um seine Privilegien zu erweitern, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Dateien zu löschen oder zu manipulieren oder einen Cross Site Scripting-Angriff durchzuführen.

- Link

—

Tue, 13 Aug 2024

[NEU] [UNGEPATCHT] [kritisch] Ivanti Connect Secure und Fortinet FortiGate: Mehrere Schwachstellen ermöglichen Manipulation von Dateien und die Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure und Fortinet FortiGate ausnutzen, um Dateien zu manipulieren und vertrauliche Informationen preiszugeben.

- Link

—

Tue, 13 Aug 2024

[NEU] [hoch] IBM VIOS und AIX: Mehrere Schwachstellen

Ein entfernter Angreifer oder ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in IBM VIOS und IBM AIX ausnutzen, um Informationen offenzulegen oder um beliebigen Code auszuführen.

- Link

—

Tue, 13 Aug 2024

[NEU] [hoch] IBM App Connect Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in IBM App Connect Enterprise ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, einen Denial of Service Zustand auszulösen und mehrere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um beliebigen Code auszuführen, einen ‘Denial of Service’-Zustand zu verursachen, seine Privilegien zu erweitern und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] QT: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in QT ausnutzen, um Informationen offenzulegen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 13 Aug 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- Link

—

Tue, 13 Aug 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 13 Aug 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Mon, 12 Aug 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- Link

—

Mon, 12 Aug 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Mon, 12 Aug 2024

[NEU] [hoch] Zabbix: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um Informationen offenzulegen, Dateien zu manipulieren, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder beliebigen Code auszuführen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/13/2024	[Amazon Linux 2 : openssl11 (ALAS-2024-2621)]	critical
8/13/2024	[Ivanti Virtual Traffic Manager (vTM) 22.2 < 22.2R1 / 22.3 < 22.3R3 / 22.5 < 22.5R2 / 22.6 < 22.6R2 / 22.7 < 22.7R2 Authentication Bypass (CVE-2024-7593)]	critical
8/13/2024	[KB5041823: Windows Server 2008 R2 Security Update (August 2024)]	critical
8/13/2024	[KB5041847: Windows Server 2008 Security Update (August 2024)]	critical
8/13/2024	[KB5041850: Windows Server 2008 Security Update (August 2024)]	critical
8/13/2024	[RHEL 7 / 8 : Red Hat JBoss Core Services Apache HTTP Server 2.4.57 SP5 (RHSA-2024:5239)]	critical
8/13/2024	[Oracle Linux 8 : wget (ELSA-2024-5299)]	critical
8/13/2024	[RHEL 8 : kernel-rt (RHSA-2024:5282)]	high
8/13/2024	[Oracle Linux 9 : bind / and / bind-dyndb-ldap (ELSA-2024-5231)]	high
8/13/2024	[FreeBSD : Vaultwarden – Multiple vulnerabilities (d2723b0f-58d9-11ef-b611-84a93843eb75)]	high

Datum	Schwachstelle	Bewertung
8/13/2024	[FreeBSD : OpenHAB CometVisu addon – Multiple vulnerabilities (587ed8ac-5957-11ef-854a-001e676bf734)]	high
8/13/2024	[Adobe Bridge 13.x < 13.0.9 / 14.x < 14.1.2 Multiple Vulnerabilities (APSB24-59)]	high
8/13/2024	[Adobe Bridge 13.x < 13.0.9 / 14.x < 14.1.2 Multiple Vulnerabilities (APSB24-59)]	high
8/13/2024	[Adobe Photoshop 24.x < 24.7.4 / 25.x < 25.11 Vulnerability (APSB24-49)]	high
8/13/2024	[Adobe Photoshop 24.x < 24.7.4 / 25.x < 25.11 Vulnerability (macOS APSB24-49)]	high
8/13/2024	[Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS : Libcroco vulnerabilities (USN-6958-1)]	high
8/13/2024	[KB5041773: Windows 10 Version 1607 / Windows Server 2016 Security Update (August 2024)]	high
8/13/2024	[KB5041585: Windows 11 version 22H2 Security Update (August 2024)]	high
8/13/2024	[Security Updates for Azure Connected Machine Agent (August 2024)]	high
8/13/2024	[KB5041592: Windows 11 version 21H2 Security Update (August 2024)]	high
8/13/2024	[KB5041580: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (August 2024)]	high
8/13/2024	[KB5041828: Windows Server 2012 R2 Security Update (August 2024)]	high
8/13/2024	[KB5041851: Windows Server 2012 Security Update (August 2024)]	high
8/13/2024	[KB5041160: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (August 2024)]	high
8/13/2024	[KB5041573: Windows 11 version 22H2 / Windows Server version 23H2 Security Update (August 2024)]	high

Datum	Schwachstelle	Bewertung
8/13/2024	[KB5041571: Windows 11 Version 24H2 Security Update (August 2024)]	high
8/13/2024	[Security Updates for Azure CycleCloud (August 2024)]	high
8/13/2024	[KB5041782: Windows 10 LTS 1507 Security Update (August 2024)]	high
8/13/2024	[KB5041578: Windows 10 version 1809 / Windows Server 2019 Security Update (August 2024)]	high
8/13/2024	[RHEL 7 : kernel (RHSA-2024:5261)]	high
8/13/2024	[RHEL 9 : kernel (RHSA-2024:5257)]	high
8/13/2024	[RHEL 8 : kernel (RHSA-2024:5281)]	high
8/13/2024	[RHEL 8 : kernel (RHSA-2024:5266)]	high
8/13/2024	[RHEL 8 : kernel (RHSA-2024:5255)]	high
8/13/2024	[IBM Java 7.1 < 7.1.5.23 / 8.0 < 8.0.8.30 Multiple Vulnerabilities]	high
8/13/2024	[IBM Java 7.1 < 7.1.5.23 / 8.0 < 8.0.8.30]	high
8/13/2024	[Ubuntu 24.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6952-2)]	high
8/13/2024	[Oracle Linux 8 : orc (ELSA-2024-5306)]	high
8/13/2024	[Oracle Linux 8 : edk2 (ELSA-2024-5297)]	high
8/13/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-6949-2)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 13 Aug 2024

WordPress MapFig Studio 0.2.1 Cross Site Request Forgery / Cross Site Scripting

WordPress MapFig Studio plugin versions 0.2.1 and below suffer from cross site request forgery and cross site scripting vulnerabilities.

- Link

—

” “Tue, 13 Aug 2024

WordPress Profilepro 1.3 Cross Site Scripting

WordPress Profilepro plugin versions 1.3 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 13 Aug 2024

WordPress Light Poll 1.0.0 Cross Site Request Forgery

WordPress Light Poll plugin versions 1.0.0 and below suffer from multiple cross site request forgery vulnerabilities.

- Link

—

” “Tue, 13 Aug 2024

WordPress PVN Auth Popup 1.0.0 Cross Site Scripting

WordPress PVN Auth Popup plugin version 1.0.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Giftora 1.0 Cross Site Request Forgery

Giftora version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Gas Agency Management 2022 Shell Upload

Gas Agency Management version 2022 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Farmacia Gama 1.0 Farmacia Gama 1.0 Cross Site Request Forgery

Farmacia Gama version 1.0 Farmacia Gama version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Employees Pay Slip PDF Generator System 1.0 Cross Site Request Forgery

Employees Pay Slip PDF Generator System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Tue, 13 Aug 2024

Bakery Shop Management System 1.0 Cross Site Request Forgery

Bakery Shop Management System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Computer Laboratory Management 1.0 SQL Injection

Computer Laboratory Management version 1.0 suffers from a remote authenticated SQL injection vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Courier Management System 2020-1.0 SQL Injection

Courier Management System version 2020-1.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

” “Mon, 12 Aug 2024

Backdoor.Win32.Nightmare.25 MVID-2024-0687 Code Execution

Backdoor.Win32.Nightmare.25 malware suffers from a code execution vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Gas Agency Management 2022 Cross Site Request Forgery

Gas Agency Management version 2022 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Garden Gate 2.6 SQL Injection

Garden Gate version 2.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 12 Aug 2024

Goati Track 1.0-2023 Insecure Settings

Gaati Track version 1.0-2023 suffers from an ignored default credential vulnerability.
- Link

—

” “Mon, 12 Aug 2024

Farmacia Gama 1.0 Insecure Direct Object Reference

Farmacia Gama version 1.0 suffers from an insecure direct object reference vulnerability.
- Link

—

” “Mon, 12 Aug 2024

Employee Management System 1.0 Insecure Settings

Employee Management System version 1.0 suffers from an ignored default credential vulnerability.
- Link

—

” “Mon, 12 Aug 2024

Computer And Mobile Repair Shop Management System 1.0 Cross Site Request Forgery

Computer and Mobile Repair Shop Management System version 1.0 suffers from a cross site request forgery vulnerability.
- Link

—

” “Fri, 09 Aug 2024

Gaati Track 1.0-2023 Insecure Direct Object Reference

Gaati Track version 1.0-2023 suffers from an insecure direct object reference vulnerability.
- Link

—

” “Fri, 09 Aug 2024

Farmacia Gama 1.0 File Inclusion

Farmacia Gama version 1.0 suffers from a file inclusion vulnerability.
- Link

—

” “Fri, 09 Aug 2024

Employee Management System 1.0 Cross Site Request Forgery

Employee Management System version 1.0 suffers from a cross site request forgery vulnerability.
- Link

—

” “Fri, 09 Aug 2024

E-Commerce Site Using PHP PDO 1.0 Cross Site Scripting

E-Commerce Site using PHP PDO version 1.0 suffers from a cross site scripting vulnerability.
- Link

—

” “Fri, 09 Aug 2024

Bhojon Restaurant Management System 2.8 Insecure Direct Object Reference

Bhojon Restaurant Management System version 2.9 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Fri, 09 Aug 2024

Xain-Hotel Management System 2.5 Insecure Settings

Xain-Hotel Management System version 2.5 suffers from an ignored default credential vulnerability.

- Link

—

” “Fri, 09 Aug 2024

Yoga Class Registration System 1.0 Cross Site Request Forgery

Yoga Class Registration System version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.

Zum Youtube Video

6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-08-11	Université Paris-Saclay	[FRA]	Link
2024-08-10	2Park	[NLD]	Link
2024-08-09	Quálitas	[MEX]	Link
2024-08-09	Schlatter Industries AG	[CHE]	Link
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	Link
2024-08-07	Killeen	[USA]	Link
2024-08-06	Nilörn	[SWE]	Link
2024-08-06	Sumter County Sheriff's Office	[USA]	Link
2024-08-05	La ville de North Miami	[USA]	Link
2024-08-05	McLaren Health Care	[USA]	Link
2024-08-04	RMN-Grand Palais	[FRA]	Link
2024-08-03	Xtrim	[ECU]	Link
2024-08-02	Ihecs	[BEL]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-14	[hugwi.ch]	helldown	Link
2024-08-14	[Patriot Machine, data leak.]	donutleaks	Link
2024-08-13	[Forrec]	blacksuit	Link
2024-08-13	[American Contract Systems]	meow	Link
2024-08-13	[Element Food Solutions]	meow	Link
2024-08-13	[Aerotech Solutions]	meow	Link
2024-08-13	[E-Z UP]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-13	[Safefood]	meow	Link
2024-08-13	[Gaston Fence]	meow	Link
2024-08-13	[Parker Development Company]	play	Link
2024-08-13	[Air International Thermal Systems]	play	Link
2024-08-13	[Adina Design]	play	Link
2024-08-13	[CinemaTech]	play	Link
2024-08-13	[Erie Meats]	play	Link
2024-08-13	[M??? ????k ??????]	play	Link
2024-08-13	[SCHLATTNER.de]	helldown	Link
2024-08-13	[deganis.fr]	helldown	Link
2024-08-13	[The White Center Community Development Association]	rhysida	Link
2024-08-13	[lenmed.co.za]	darkvault	Link
2024-08-13	[gpf.org.za]	darkvault	Link
2024-08-13	[Banner and Associates]	trinity	Link
2024-08-13	[Southwest Family Medicine Associates]	bianlian	Link
2024-08-13	[glazkov.co.il]	darkvault	Link
2024-08-05	[XPERT Business Solutions GmbH]	helldown	Link
2024-08-05	[MyFreightWorld]	helldown	Link
2024-08-09	[cbmm.org]	helldown	Link
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	Link
2024-08-11	[briju.pl]	helldown	Link
2024-08-11	[vindix.pl]	helldown	Link
2024-08-11	[Albatros S.r.l.]	helldown	Link
2024-08-12	[NetOne]	hunters	Link
2024-08-12	[fabamaq.com]	BrainCipher	Link
2024-08-12	[cyceron.fr]	BrainCipher	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-12	[bedford.k12.oh.us]	ransomhub	Link
2024-08-12	[Warwick Hotels and Resorts]	lynx	Link
2024-08-12	[VVS-Eksperten]	cicada3301	Link
2024-08-12	[Brookshire Dental]	qilin	Link
2024-08-07	[Alvan Blanch Development]	lynx	Link
2024-08-11	[parkerdevco.com]	dispossessor	Link
2024-08-11	[naturalcuriosities.com]	ransomhub	Link
2024-08-11	[TelPro]	play	Link
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	Link
2024-08-11	[Amco Metal Industrial Corporation]	qilin	Link
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	Link
2024-08-11	[Moser Wealth Advisors]	rhysida	Link
2024-08-09	[alliuminteriors.co.nz]	ransomhub	Link
2024-08-11	[robertshvac.com]	abyss	Link
2024-08-11	[dmmerch.com]	lockbit3	Link
2024-08-11	[luisoliveras.com]	lockbit3	Link
2024-08-11	[legacycpas.com]	lockbit3	Link
2024-08-11	[allweatheraa.com]	lockbit3	Link
2024-08-11	[soprema.com]	lockbit3	Link
2024-08-11	[exol-lubricants.com]	lockbit3	Link
2024-08-11	[fremontschools.net]	lockbit3	Link
2024-08-11	[acdcexpress.com]	lockbit3	Link
2024-08-11	[clinicatezza.com.pe]	lockbit3	Link
2024-08-11	[divaris.com]	lockbit3	Link
2024-08-11	[sullivansteelservice.com]	lockbit3	Link
2024-08-11	[johnllowery.com]	lockbit3	Link
2024-08-11	[qespavements.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-11	[emanic.net]	lockbit3	Link
2024-08-11	[Hanon Systems]	hunters	Link
2024-08-10	[kronospublic.com]	lockbit3	Link
2024-08-10	[Brontoo Technology Solutions]	ransomexx	Link
2024-08-07	[Cydcor]	dragonforce	Link
2024-08-09	[Credible Group]	play	Link
2024-08-09	[Nilorngruppen AB]	play	Link
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	Link
2024-08-09	[Anniversary Holding Company]	bianlian	Link
2024-08-09	[GCA Global Cargo Alliance]	bianlian	Link
2024-08-09	[Majestic Metals]	bianlian	Link
2024-08-09	[dhcgrp.com]	ransomhub	Link
2024-08-05	[Boombah Inc.]	incransom	Link
2024-08-09	[www.dunnsolutions.com]	dAn0n	Link
2024-08-09	[Sumter County Sheriff]	rhysida	Link
2024-08-06	[pierrediamonds.com.au]	ransomhub	Link
2024-08-08	[golfoy.com]	ransomhub	Link
2024-08-08	[inv-dar.com]	ransomhub	Link
2024-08-08	[icarasia.com]	killsec	Link
2024-08-08	[rationalenterprise.com]	ransomhub	Link
2024-08-02	[modernceramics.com]	ransomhub	Link
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-08	[tibaitservices.com]	cactus	Link
2024-08-08	[mihlfeld.com]	cactus	Link
2024-08-08	[Horizon View Medical Center]	everest	Link
2024-08-08	[comoferta.com]	darkvault	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-08	[NIDEC CORPORATION]	everest	Link
2024-08-08	[mercadomineiro.com.br]	darkvault	Link
2024-08-07	[hudsoncivil.com.au]	ransomhub	Link
2024-08-07	[www.jgsummit.com.ph]	ransomhub	Link
2024-08-07	[Bayhealth Hospital]	rhysida	Link
2024-08-07	[amplicon.com]	ransomhub	Link
2024-08-06	[infotexim.pe]	ransomhub	Link
2024-08-07	[suandco.com]	madliberator	Link
2024-08-07	[Anderson Oil & Gas]	hunters	Link
2024-08-07	[bonatra.com]	killsec	Link
2024-08-07	[FatBoy Cellular]	meow	Link
2024-08-07	[KLA]	meow	Link
2024-08-07	[HUD User]	meow	Link
2024-08-06	[msprocuradores.es]	madliberator	Link
2024-08-06	[www.carri.com]	alphalocker	Link
2024-08-06	[www.consorzioinnova.it]	alphalocker	Link
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-06	[biw-burger.de]	alphalocker	Link
2024-08-06	[www.sobha.com]	ransomhub	Link
2024-08-06	[Alternate Energy]	play	Link
2024-08-06	[True Blue Environmental]	play	Link
2024-08-06	[Granit Design]	play	Link
2024-08-06	[KinetX]	play	Link
2024-08-06	[Omni Family Health]	hunters	Link
2024-08-06	[IOI Corporation Berhad]	fog	Link
2024-08-06	[Ziba Design]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-06	[Casco Antiguo]	hunters	Link
2024-08-06	[Fractalia Group]	hunters	Link
2024-08-06	[Banx Systems]	meow	Link
2024-08-05	[Silipos]	cicada3301	Link
2024-08-04	[kierlcpa.com]	lockbit3	Link
2024-08-05	[Square One Coating Systems]	cicada3301	Link
2024-08-05	[Hi-P International]	fog	Link
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	Link
2024-08-05	[HP Distribution]	incransom	Link
2024-08-05	[exco-solutions.com]	cactus	Link
2024-08-05	[Maryville Academy]	rhysida	Link
2024-08-04	[notariusze.waw.pl]	killsec	Link
2024-08-04	[Ranney School]	rhysida	Link
2024-08-03	[nursing.com]	ransomexx	Link
2024-08-03	[Bettis Asphalt]	blacksuit	Link
2024-08-03	[fcl.crs]	lockbit3	Link
2024-08-03	[CPA Tax Solutions]	meow	Link
2024-08-03	[LRN]	hunters	Link
2024-08-03	[aikenhousing.org]	blacksuit	Link
2024-08-02	[David E Shambach Architect]	dragonforce	Link
2024-08-02	[Hayes Beer Distributing]	dragonforce	Link
2024-08-02	[Jangho Group]	hunters	Link
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	Link
2024-08-02	[retaildatallc.com]	ransomhub	Link
2024-08-02	[WPG Holdings]	meow	Link
2024-08-02	[National Beverage]	meow	Link
2024-08-02	[PeoplesHR]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-02	[Dometic Group]	meow	Link
2024-08-02	[Remitano]	meow	Link
2024-08-02	[Premier Equities]	meow	Link
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	Link
2024-08-02	[q-cells.de]	abyss	Link
2024-08-02	[coinbv.nl]	madliberator	Link
2024-08-01	[Valley Bulk]	cicada3301	Link
2024-08-01	[ENEA Italy]	hunters	Link
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	Link
2024-08-01	[effinghamschools.com]	ransomhub	Link
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	Link
2024-08-01	[Adorna & Guzman Dentistry]	monti	Link
2024-08-01	[Camp Susque]	medusa	Link
2024-08-01	[Ali Gohar]	medusa	Link
2024-08-01	[acsi.org]	blacksuit	Link
2024-08-01	[County Linen UK]	dispossessor	Link
2024-08-01	[TNT Materials tnt-materials.com/]	dispossessor	Link
2024-08-01	[Peñoles]	akira	Link
2024-08-01	[dahlvalve.com]	cactus	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.