Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240803

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

Unbefugte Zugriffe auf IT-Managementlösung Aruba ClearPass möglich

Die Entwickler von HPE Aruba Networking haben in ClearPass Policy Manager unter anderem eine kritische Sicherheitslücke geschlossen.

- Link

—

Kritische Sicherheitslücke bedroht Google Chrome

Angreifer können an mehreren Schwachstellen in Chrome ansetzen, um PCs zu kompromittieren.

- Link

—

Keine Sicherheitsupdates in Sicht: Avast Free Antivirus ist verwundbar

Sicherheitsforscher warnen vor Schwachstellen in Avast Free Antivirus und raten aufgrund fehlender Patches von einer Nutzung ab.

- Link

—

Jetzt patchen! Ransomware-Attacken auf VMware ESXi-Server beobachtet

Sicherheitsforscher warnen vor laufenden Attacken auf Systeme mit ESXi-Hypervisor. Darüber gelangen Erpressungstrojaner auf Computer.

- Link

—

Selenium Grid: Unsichere Standardkonfiguration lässt Krypto-Miner passieren

Das Framework für automatisierte Softwaretests Selenium Grid ist in den Standardeinstellungen verwundbar. Das nutzen Angreifer derzeit aus.

- Link

—

Angreifer nutzen Schadcode-Lücke in Acronis Cyber Infrastructure aus

In mehreren aktualisierten Versionen von Acronis Cyber Infrastructure haben die Entwickler eine kritische Lücke geschlossen.

- Link

—

Sicherheitsupdate schützt SolarWinds Platform vor möglichen Attacken

Angreifer können die IT-Verwaltungssoftware SolarWinds Platform attackieren. Die Entwickler haben mehrere Schwachstellen geschlossen.

- Link

—

Sicherheitslücke: Entwickler raten zum zügigen Patchen von Telerik Report Server
Ein wichtiges Sicherheitsupdate schließt eine kritische Lücke in der IT-Management- und Reportinglösung Telerik Report Server.
- Link

—

Jetzt patchen! Angreifer attackieren Now Platform von ServiceNow
Die Cloud Computing Plattform von ServiceNow ist derzeit im Visier von Angreifern und sie nutzen kritische Sicherheitslücken aus.
- Link

—

Sicherheitsupdates: Aruba EdgeConnect SD-WAN vielfältig attackierbar
Die Entwickler von HPE haben in Arubas SD-WAN-Lösung EdgeConnect mehrere gefährliche Sicherheitslücken geschlossen.
- 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	0.988500000	Link
CVE-2023-6895	0.922010000	0.989880000	Link
CVE-2023-6553	0.925190000	0.990280000	Link
CVE-2023-5360	0.903980000	0.988570000	Link
CVE-2023-52251	0.940460000	0.991870000	Link
CVE-2023-4966	0.971710000	0.998360000	Link
CVE-2023-49103	0.962110000	0.995470000	Link
CVE-2023-48795	0.964660000	0.996100000	Link
CVE-2023-47246	0.957550000	0.994650000	Link
CVE-2023-46805	0.936080000	0.991380000	Link
CVE-2023-46747	0.972730000	0.998760000	Link
CVE-2023-46604	0.961790000	0.995410000	Link
CVE-2023-4542	0.928310000	0.990550000	Link
CVE-2023-43208	0.965360000	0.996360000	Link
CVE-2023-43177	0.965600000	0.996430000	Link
CVE-2023-42793	0.970370000	0.997870000	Link
CVE-2023-41265	0.911110000	0.989050000	Link
CVE-2023-39143	0.941900000	0.992070000	Link
CVE-2023-38646	0.906610000	0.988750000	Link
CVE-2023-38205	0.954590000	0.994110000	Link
CVE-2023-38203	0.966410000	0.996630000	Link
CVE-2023-38035	0.974680000	0.999700000	Link
CVE-2023-36845	0.964250000	0.996010000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965340000	0.996350000	Link
CVE-2023-35082	0.968030000	0.997130000	Link
CVE-2023-35078	0.970390000	0.997870000	Link
CVE-2023-34993	0.972880000	0.998840000	Link
CVE-2023-34960	0.936550000	0.991440000	Link
CVE-2023-34634	0.930910000	0.990850000	Link
CVE-2023-34468	0.906650000	0.988750000	Link
CVE-2023-34362	0.969450000	0.997540000	Link
CVE-2023-34039	0.944910000	0.992510000	Link
CVE-2023-3368	0.935570000	0.991320000	Link
CVE-2023-33246	0.972140000	0.998540000	Link
CVE-2023-32315	0.973620000	0.999150000	Link
CVE-2023-30625	0.948260000	0.993030000	Link
CVE-2023-30013	0.962790000	0.995630000	Link
CVE-2023-29300	0.968930000	0.997360000	Link
CVE-2023-29298	0.943640000	0.992330000	Link
CVE-2023-28343	0.923780000	0.990100000	Link
CVE-2023-28121	0.909500000	0.988930000	Link
CVE-2023-27524	0.970600000	0.997960000	Link
CVE-2023-27372	0.973190000	0.998980000	Link
CVE-2023-27350	0.969960000	0.997730000	Link
CVE-2023-26469	0.956500000	0.994480000	Link
CVE-2023-26360	0.959350000	0.994950000	Link
CVE-2023-26035	0.967950000	0.997100000	Link
CVE-2023-25717	0.954090000	0.993990000	Link
CVE-2023-25194	0.968820000	0.997350000	Link
CVE-2023-2479	0.963740000	0.995870000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.973540000	0.999110000	Link
CVE-2023-23752	0.956380000	0.994460000	Link
CVE-2023-23333	0.958950000	0.994870000	Link
CVE-2023-22527	0.968290000	0.997180000	Link
CVE-2023-22518	0.964890000	0.996150000	Link
CVE-2023-22515	0.973730000	0.999210000	Link
CVE-2023-21839	0.957210000	0.994570000	Link
CVE-2023-21554	0.952830000	0.993750000	Link
CVE-2023-20887	0.970170000	0.997790000	Link
CVE-2023-1698	0.910560000	0.989020000	Link
CVE-2023-1671	0.962480000	0.995550000	Link
CVE-2023-0669	0.969440000	0.997520000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 02 Aug 2024

[NEU] [hoch] Microsoft Dynamics 365: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft Dynamics 365 ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um Informationen offenzulegen oder beliebigen Programmcode auszuführen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] Apache Tomcat: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in Apache Tomcat ausnutzen, um seine Privilegien zu

erhöhen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [kritisch] Apache Tomcat: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM MQ ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen oder einen unspezifischen Angriff durchzuführen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Fri, 02 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um

beliebigen Code auszuführen oder einen ‘Denial of Service’-Zustand zu verursachen.
- Link

—

Fri, 02 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

—

Fri, 02 Aug 2024

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.
- Link

—

Fri, 02 Aug 2024

[NEU] [hoch] Rockwell Automation ControlLogix: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Rockwell Automation ControlLogix ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] expat: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in expat ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] Broadcom Brocade Switch: Mehrere Schwachstellen

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Broadcom Brocade

Switch und Broadcom Fabric OS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen und vertrauliche Informationen preiszugeben.

- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Thu, 01 Aug 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 01 Aug 2024

[NEU] [hoch] xwiki: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in xwiki ausnutzen, um Sicherheitsvorkehrungen zu umgehen, einen Cross-Site-Scripting-Angriff durchzuführen und beliebigen Code auszuführen.

- Link

—

Thu, 01 Aug 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 01 Aug 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/2/2024	[OSGeo GeoTools RCE (CVE-2024-36404)]	critical
8/2/2024	[OSGeo GeoServer RCE (CVE-2024-36401)]	critical
8/1/2024	[Danswer Unauthenticated Access]	critical
8/1/2024	[GeoServer Remote Code Execution]	critical
8/1/2024	[Oracle Linux 9 : freeradius (ELSA-2024-4935)]	critical
8/1/2024	[Rocky Linux 9 : freeradius (RLSA-2024:4935)]	critical
8/1/2024	[Ubuntu 14.04 LTS : Apache Commons Collections vulnerability (USN-6936-1)]	critical
8/1/2024	[Fedora 40 : kernel (2024-873e2cb5f2)]	critical
8/1/2024	[Amazon Linux 2 : docker (ALASDOCKER-2024-040)]	critical
8/1/2024	[FreeBSD : chromium – multiple security fixes (15d398ea-4f73-11ef-8a0f-a8a1599412c6)]	critical
8/1/2024	[RHEL 8 : emacs (RHSA-2024:4971)]	critical
8/1/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Gross vulnerability (USN-6942-1)]	critical
8/1/2024	[Amazon Linux 2023 : docker (ALAS2023-2024-674)]	critical
7/31/2024	[RHEL 7 : httpd (RHSA-2024:4943)]	critical
7/31/2024	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2024-041)]	critical
8/2/2024	[Photon OS 5.0: Python3 PHSA-2024-5.0-0338]	high
8/2/2024	[ImageMagick < 7.11-36 Arbitrary Code Execution]	high
8/2/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-6895-4)]	high
8/2/2024	[Progress MOVEit Transfer < 2023.0.12 / 2023.1 < 2023.1.7 / 2024.0 < 2024.0.3 Privilege Escalation]	high
8/2/2024	[ManageEngine OpManager SQLi (CVE-2024-6748)]	high
8/1/2024	[Photon OS 4.0: Python3 PHSA-2024-4.0-0660]	high
8/1/2024	[Fedora 40 : obs-cef (2024-47dbf2a4de)]	high

Datum	Schwachstelle	Bewertung
8/1/2024	[Slackware Linux 15.0 / current curl Vulnerability (SSA:2024-213-01)]	high
8/1/2024	[RHEL 8 : kpatch-patch-4_18_0-305_120_1 (RHSA-2024:4970)]	high
8/1/2024	[Ubuntu 14.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6926-2)]	high
8/1/2024	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.5.6.5)]	high
8/1/2024	[Ubuntu 18.04 LTS : Bind vulnerabilities (USN-6909-2)]	high
8/1/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Tomcat vulnerabilities (USN-6943-1)]	high
7/31/2024	[SUSE SLES12 Security Update : gvfs (SUSE-SU-2024:2681-1)]	high
7/31/2024	[Panasonic WV-S2231L Camera Denial of Service (CVE-2020-29194)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 02 Aug 2024

Packet Storm New Exploits For July, 2024

This archive contains all of the 105 exploits added to Packet Storm in July, 2024.

- Link

—

” “Fri, 02 Aug 2024

Tourism Management System 2.0 Cross Site Scripting

Tourism Management System version 2.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 02 Aug 2024

Computer Laboratory Management System 1.0 Privilege Escalation

Computer Laboratory Management System version 1.0 suffers from an incorrect access control that

allows for privilege escalation.

- Link

—

” “Fri, 02 Aug 2024

Leads Manager Tool SQL Injection / Cross Site Scripting

Leads Manager Tool suffers from remote SQL injection and cross site scripting vulnerabilities.

- Link

—

” “Fri, 02 Aug 2024

ReadyMade Unilevel Ecommerce MLM Blind SQL Injection / Cross Site Scripting

Readymade Unilevel Ecommerce MLM suffers from remote blind SQL injection and cross site scripting vulnerabilities. These issues affected the version released as late as March 15, 2024.

- Link

—

” “Fri, 02 Aug 2024

Appointment Scheduler 3.0 Insecure Direct Object Reference

Appointment Scheduler version 3.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Fri, 02 Aug 2024

AccPack Cop 1.0 Cross Site Request Forgery

AccPack Cop version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Fri, 02 Aug 2024

AccPack Buzz 1.0 SQL Injection

AccPack Buzz version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 01 Aug 2024

Availability Calendar 5.0 Insecure Direct Object Reference

Availability Calendar version 5.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Thu, 01 Aug 2024

Oracle Database 12c Release 1 Unquoted Service Path

Oracle Database version 12c Release 1 suffers from an unquoted service path vulnerability.

- Link

—

” “Thu, 01 Aug 2024

SolarWinds Kiwi Syslog Server 9.6.7.1 Unquoted Service Path

SolarWinds Kiwi Syslog Server version 9.6.7.1 suffers from an unquoted service path vulnerability.

- Link

—

” “Thu, 01 Aug 2024

Babaji E-Commerce 1.0 Insecure Settings

Babaji E-Commerce version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 31 Jul 2024

OpenMediaVault rpc.php Authenticated Cron Remote Code Execution

OpenMediaVault allows an authenticated user to create cron jobs as root on the system. An attacker can abuse this by sending a POST request via rpc.php to schedule and execute a cron entry that runs arbitrary commands as root on the system. All OpenMediaVault versions including the latest release 7.4.2-2 are vulnerable.

- Link

—

” “Wed, 31 Jul 2024

Readymade Real Estate Script SQL Injection / Cross Site Scripting

Readymade Real Estate Script suffers from remote blind SQL injection and cross site scripting vulnerabilities. This was last validated on the build available as of July 12, 2024.

- Link

—

” “Wed, 31 Jul 2024

AMPLE BILLS 1.0 Cross Site Scripting

AMPLE BILLS version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 31 Jul 2024

Aero CMS 0.0.1 Cross Site Request Forgery

Aero CMS version 0.0.1 suffers from a cross site request forgery vulnerability.

- Link

—

” “Wed, 31 Jul 2024

SchoolPlus LMS 1.0 SQL Injection

SchoolPlus LMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 31 Jul 2024

AccPack Khanepani 1.0 Insecure Direct Object Reference

AccPack Khanepani version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 31 Jul 2024

AccPack Cop 1.0 SQL Injection

AccPack Cop version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 31 Jul 2024

AccPack Buzz 1.0 Arbitrary File Upload

AccPack Buzz version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 31 Jul 2024

Academy LMS 6.8.1 Cross Site Scripting

Academy LMS version 6.8.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 30 Jul 2024

Chuksrio LMS 2.9 Insecure Direct Object Reference

Chuksrio LMS version 2.9 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Tue, 30 Jul 2024

AMPLE BILLS 1.0 Administrative Page Disclosure

AMPLE BILLS version 1.0 appears to suffer from an administrative page disclosure issue.

- Link

—

” “Tue, 30 Jul 2024

SchoolPlus 1.0 Shell Upload

SchoolPlus version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 30 Jul 2024

AccPack Khanepani 1.0 SQL Injection

AccPack Khanepani version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 01 Aug 2024

ZDI-24-1053: (0Day) (Pwn2Own) ChargePoint Home Flex OCPP bswitch Command Injection Remote Code Execution Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1052: (0Day) (Pwn2Own) ChargePoint Home Flex Improper Certificate Validation Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1051: (0Day) (Pwn2Own) ChargePoint Home Flex wlanchnllst Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1050: (0Day) (Pwn2Own) ChargePoint Home Flex SrvrToSmSetAutoChnlListMsg Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1049: (0Day) (Pwn2Own) ChargePoint Home Flex wlanapp Command Injection Remote Code Execution Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1048: (0Day) (Pwn2Own) ChargePoint Home Flex onboardee Improper Access Control

Remote Code Execution Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1047: (0Day) ChargePoint Home Flex Bluetooth Low Energy Denial-of-Service Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1046: (0Day) ChargePoint Home Flex Bluetooth Low Energy Information Disclosure Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1045: (0Day) (Pwn2Own) Pioneer DMH-WT7600NEX Telematics Improper Certificate Validation Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1044: (0Day) (Pwn2Own) Pioneer DMH-WT7600NEX Telematics Directory Traversal Arbitrary File Creation Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1043: (0Day) (Pwn2Own) Pioneer DMH-WT7600NEX Media Service Improper Handling of Exceptional Conditions Denial-of-Service Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1042: NoMachine Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

- Link

—

” “Thu, 01 Aug 2024

ZDI-24-1041: Google Chrome Updater DosDevices Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1040: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerabi-

lity

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1039: PaperCut NG web-print-hot-folder Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1038: PaperCut NG pc-web-print Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1037: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1036: Check Point ZoneAlarm Extreme Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1035: Microsoft Windows NTFS Junction Heap-based Buffer Overflow Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1034: Oracle VirtualBox EHCI USB Controller Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1033: NI FlexLogger Redis Server Incorrect Permission Assignment Information Disclosure Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1032: NI FlexLogger Redis Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1031: NI VeriStand NIVSPRJ File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1030: NI VeriStand VSMODEL File Parsing Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1029: NI VeriStand DataLoggingServer Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1028: NI VeriStand WaveformStreamingServer Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1027: NI VeriStand ProjectServer OpenTool Exposed Dangerous Method Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1026: NI VeriStand ProjectServer Exposed Dangerous Method Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1025: NI VeriStand IFileTransferServer Exposed Dangerous Method Information Disclosure Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1024: NI VeriStand ProjectServer Exposed Dangerous Method Denial-of-Service Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1023: Trend Micro VPN Proxy One Pro Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1022: Trend Micro VPN Proxy One Pro Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1021: Logsign Unified SecOps Platform Directory Traversal Information Disclosure Vulnerability

- Link

—

”

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

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.