Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240802

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

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 Reporting-lösung 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

—

Docker: Alte Sicherheitslücke zur Rechteausweitung wieder aufgetaucht

Eine Schwachstelle in den Autorisierung-Plug-ins hatte Docker 2019 geschlossen. Sie ist aber kurz danach als Regression wieder in die Engine eingeflossen.

- 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	0.988640000	Link
CVE-2023-6895	0.922010000	0.990000000	Link
CVE-2023-6553	0.937510000	0.991640000	Link
CVE-2023-5360	0.903980000	0.988700000	Link
CVE-2023-52251	0.940460000	0.991960000	Link
CVE-2023-4966	0.971710000	0.998380000	Link
CVE-2023-49103	0.953130000	0.993900000	Link
CVE-2023-48795	0.964660000	0.996150000	Link
CVE-2023-47246	0.957550000	0.994710000	Link
CVE-2023-46805	0.936080000	0.991470000	Link
CVE-2023-46747	0.972730000	0.998770000	Link
CVE-2023-46604	0.961790000	0.995480000	Link
CVE-2023-4542	0.928310000	0.990650000	Link
CVE-2023-43208	0.965360000	0.996410000	Link
CVE-2023-43177	0.965600000	0.996480000	Link
CVE-2023-42793	0.970370000	0.997900000	Link
CVE-2023-41265	0.911110000	0.989180000	Link
CVE-2023-39143	0.941900000	0.992160000	Link
CVE-2023-38646	0.906610000	0.988880000	Link
CVE-2023-38205	0.954590000	0.994190000	Link
CVE-2023-38203	0.966410000	0.996670000	Link
CVE-2023-38035	0.974400000	0.999580000	Link
CVE-2023-36845	0.964250000	0.996060000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965340000	0.996400000	Link
CVE-2023-35082	0.968030000	0.997160000	Link
CVE-2023-35078	0.970390000	0.997910000	Link
CVE-2023-34993	0.972880000	0.998850000	Link
CVE-2023-34960	0.936550000	0.991540000	Link
CVE-2023-34634	0.930910000	0.990950000	Link
CVE-2023-34468	0.906650000	0.988890000	Link
CVE-2023-34362	0.969450000	0.997570000	Link
CVE-2023-34039	0.944910000	0.992600000	Link
CVE-2023-3368	0.935570000	0.991410000	Link
CVE-2023-33246	0.972610000	0.998720000	Link
CVE-2023-32315	0.973620000	0.999160000	Link
CVE-2023-30625	0.948260000	0.993130000	Link
CVE-2023-30013	0.962790000	0.995700000	Link
CVE-2023-29300	0.968930000	0.997400000	Link
CVE-2023-29298	0.943640000	0.992420000	Link
CVE-2023-28343	0.923780000	0.990210000	Link
CVE-2023-28121	0.909500000	0.989050000	Link
CVE-2023-27524	0.970600000	0.997990000	Link
CVE-2023-27372	0.973190000	0.998990000	Link
CVE-2023-27350	0.969960000	0.997760000	Link
CVE-2023-26469	0.956500000	0.994550000	Link
CVE-2023-26360	0.959350000	0.995020000	Link
CVE-2023-26035	0.967950000	0.997140000	Link
CVE-2023-25717	0.954090000	0.994070000	Link
CVE-2023-25194	0.968820000	0.997380000	Link
CVE-2023-2479	0.963740000	0.995920000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.973540000	0.999130000	Link
CVE-2023-23752	0.960260000	0.995180000	Link
CVE-2023-23333	0.958950000	0.994940000	Link
CVE-2023-22527	0.968290000	0.997230000	Link
CVE-2023-22518	0.964890000	0.996210000	Link
CVE-2023-22515	0.973730000	0.999220000	Link
CVE-2023-21839	0.957210000	0.994640000	Link
CVE-2023-21554	0.952830000	0.993830000	Link
CVE-2023-20887	0.970170000	0.997830000	Link
CVE-2023-1698	0.910560000	0.989140000	Link
CVE-2023-1671	0.962480000	0.995610000	Link
CVE-2023-0669	0.969440000	0.997550000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

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

—

Thu, 01 Aug 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Denial of Service

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen Denial of Service Angriff

durchzuführen oder um Informationen offenzulegen.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Codeausführung und DoS

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.
- Link

—

Thu, 01 Aug 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 01 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

—

Thu, 01 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

—

Thu, 01 Aug 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Exim ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 01 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

—

Thu, 01 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
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	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : apache2 (SUSE-SU-2024:2624-1)]	critical
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : git (SUSE-SU-2024:2656-1)]	critical
7/31/2024	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2024-041)]	critical
8/1/2024	[Photon OS 4.0: Python3 PHSA-2024-4.0-0660]	high
8/1/2024	[Fedora 40 : obs-cef (2024-47dbf2a4de)]	high
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

Datum	Schwachstelle	Bewertung
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 : orc (SUSE-SU-2024:2643-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : java-11-openjdk (SUSE-SU-2024:2629-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gtk2 (SUSE-SU-2024:2634-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : orc (SUSE-SU-2024:2663-1)]	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

“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.

- 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

—

” “Tue, 30 Jul 2024

AccPack Cop CMS 1.0 SQL Injection

AccPack Cop CMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 30 Jul 2024

AccPack Buzz Cop 1.0 Cross Site Request Forgery

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

- Link

—

” “Mon, 29 Jul 2024

mySCADA MyPRO Authenticated Command Injection

An authenticated command injection vulnerability exists in MyPRO versions 8.28.0 and below from mySCADA. The vulnerability can be exploited by a remote attacker to inject arbitrary operating system commands which will get executed in the context of NT AUTHORITY\SYSTEM.

- Link

—

” “Mon, 29 Jul 2024

Blog Site 1.0 SQL Injection

Blog Site version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 29 Jul 2024

QuickJob 6.1 Insecure Settings

QuickJob version 6.1 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

Prison Management System version 1.0 Insecure Settings

Prison Management System version version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

PowerVR _DevmemXReservationPageAddress() Wrapping Addition Error

PowerVR has an issue where wrapping addition in _DevmemXReservationPageAddress() causes an MMU operation at the wrong address.

- Link

—

” “Mon, 29 Jul 2024

PowerVR DevmemXIntMapPages() / DevmemXIntUnmapPages() Integer Overflows

PowerVR has integer overflows in DevmemXIntMapPages() and DevmemXIntUnmapPages(), exploitable as dangling GPU page table entries.

- Link

—

” “Mon, 29 Jul 2024

PowerVR PMR Physical Memory Handling Flaw

PowerVR PMR allows physical memory to be freed before GPU TLB invalidation.

- Link

—

” “Mon, 29 Jul 2024

Pharmacy Management System 1.0 Insecure Settings

Pharmacy Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

Online Payment Hub System 1.0 Insecure Settings

Online Payment Hub System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

Innue Business Live Chat 2.5 Insecure Settings

Innue Business Live Chat version 2.5 suffers from an ignored default credential vulnerability.

- 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 Vulnerability

- 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

—

” “Mon, 29 Jul 2024

ZDI-24-1020: SolarWinds Access Rights Manager deleteTransferFile Directory Traversal Arbitrary File Deletion and Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1019: (Pwn2Own) Docker Desktop extension-manager Exposed Dangerous Function Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1018: (Pwn2Own) Linux Kernel io_uring Buffer List Race Condition Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1017: (0Day) Panda Security Dome Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1016: (0Day) Panda Security Dome Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1015: (0Day) Panda Security Dome VPN Incorrect Permission Assignment Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1014: (0Day) Panda Security Dome VPN DLL Hijacking Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1013: (0Day) Panda Security Dome Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1012: (0Day) F-Secure Total Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1011: (0Day) VIPRE Advanced Security SBAMSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1010: (0Day) VIPRE Advanced Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1009: (0Day) AVG AntiVirus Free icarus Arbitrary File Creation Denial of Service Vulnerabi-

lity

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1008: (0Day) AVG AntiVirus Free AVGSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1007: (0Day) AVG AntiVirus Free AVGSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1006: (0Day) AVG AntiVirus Free Link Following Denial-of-Service Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1005: (0Day) Avast Free Antivirus AvastSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1004: (0Day) Avast Free Antivirus AvastSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1003: (0Day) Avast Free Antivirus AvastSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1002: (0Day) Avast Cleanup Premium Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1001: (0Day) Avast Cleanup Premium Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1000: (0Day) Avast Cleanup Premium Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-999: (0Day) Avast Free Antivirus Link Following Denial-of-Service Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-998: KernelCI SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-997: Linux Kernel CIFS Filesystem Decryption Improper Input Validation Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-996: Linux Kernel ksmbd ACL Inheritance Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-995: Linux Kernel Netfilter Conntrack Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-994: Linux Kernel QXL VGA Driver Race Condition Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-993: Microsoft Azure myapiendpoint.developer.azure-api Improper Access Control Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-992: Microsoft Azure VSTS CLI vstscli Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-991: Microsoft Azure Arc Jumpstart Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-990: Microsoft 3D Builder GLB File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-989: Microsoft Azure Container Network Management sbidprod Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-988: Microsoft Azure MQTT azure-iot-sdks-ci Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-987: Microsoft Object Detection Solution Accelerator csaddevamlacr Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-986: Microsoft Azure IoT Edge Dev Tool iotedgetoolscontainerregistry Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-985: Microsoft Azure Service Fabric servicefabricsdkstorage Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-984: Microsoft Word DOC File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-983: Microsoft Azure Go Labs microsoftgoproxy Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-982: Microsoft Azure SQL Workshop azuremlsampleexperiments Uncontrolled Search Path Element Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-981: Microsoft Azure Machine Learning Notebooks azuremlpackages Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-980: Microsoft Azure Machine Learning Forecasting Toolkit azuremlftkrelease Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-979: Microsoft Office Visio DXF File Parsing Integer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-978: Microsoft PC Manager Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-977: Microsoft Office Excel XLW File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-976: Microsoft Office PowerPoint GLB File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-975: Microsoft Excel FBX File Parsing Use-After-Free 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
2024-08-01	[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.