Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240711

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

VMware stopft SQL-Injection-Lücke in Aria Automation

Angreifer können eine Schwachstelle in VMware Aria Automation missbrauchen, um eigene Befehle mittels SQL-Injection einzuschleusen. Updates stehen bereit.

- Link

—

Blast-RADIUS: Sicherheitslücke im Netzwerkprotokoll RADIUS veröffentlicht

Lange bekannte Schwachstellen können dem RADIUS-Protokoll zum Verhängnis werden, das vor allem im Enterprise-Umfeld in sehr vielen Netzwerken eingesetzt wird.

- Link

—

Patchday Fortinet: FortiAIOps und FortiOS gegen mögliche Attacken gerüstet

Angreifer können mehrere Produkte von Fortinet ins Visier nehmen und unter anderem sensible Daten einsehen.

- Link

—

OpenSSH: Weitere RegreSSHion-artige Lücke entdeckt

Die RegreSSHion-Lücke ermöglichte Angreifern Root-Zugriff. Ein IT-Forscher hat eine weitere ähnliche Lücke in OpenSSH von RHEL 9 und Abkömmlingen entdeckt.

- Link

—

Citrix stopft teils kritische Sicherheitslücken in mehreren Produkten

Citrix hat Sicherheitswarnungen zu mehreren Produkten veröffentlicht. Updates schließen teils kritische Schwachstellen darin.

- Link

—

Patchday Microsoft: Angreifer attackieren Windows 11 über Hyper-V

Derzeit nutzen Angreifer zwei Sicherheitslücken in verschiedenen Windows- und Windows-Server-Versionen aus. Zwei weitere Lücken sind öffentlich bekannt.

- Link

—

Patchday Adobe: Schadcode-Attacken auf InDesign & Co. möglich

Sicherheitsupdates schützen Adobe Bridge, InDesign und Premiere Pro davor, dass Angreifer eigenen Code ausführen können.

- Link

—

Patchday: SAP rüstet Unternehmenssoftware gegen etwaige Angriffe

Es sind wichtige Sicherheitsupdates unter anderem für SAP Commerce und NetWeaver erschienen.

- Link

—

Wordpress-Plug-in mit 150.000 Installation ermöglicht beliebige Dateiuploads

In einem Wordpress-Plug-in mit 150.000 Installationen wurde eine Sicherheitslücke entdeckt, die das Hochladen beliebiger Dateien erlaubt.

- Link

—

IT-Sicherheitslösung Trend Micro Apex One vor möglichen Attacken abgesichert

Angreifer können Windows-PCs mit Trend Micro Apex One oder Apex One as a Service attackieren. Sicherheitspatches sind erschienen.

- 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	0.962510000	0.995500000	Link
CVE-2023-6895	0.920390000	0.989670000	Link
CVE-2023-6553	0.936860000	0.991410000	Link
CVE-2023-5360	0.911260000	0.988980000	Link
CVE-2023-52251	0.930900000	0.990780000	Link
CVE-2023-4966	0.971290000	0.998130000	Link
CVE-2023-49103	0.953130000	0.993790000	Link
CVE-2023-48795	0.962520000	0.995510000	Link
CVE-2023-47246	0.951210000	0.993460000	Link
CVE-2023-46805	0.958670000	0.994740000	Link
CVE-2023-46747	0.972630000	0.998620000	Link
CVE-2023-46604	0.963510000	0.995770000	Link
CVE-2023-4542	0.924200000	0.990090000	Link
CVE-2023-43208	0.959520000	0.994910000	Link
CVE-2023-43177	0.962660000	0.995540000	Link
CVE-2023-42793	0.970470000	0.997780000	Link
CVE-2023-41265	0.905890000	0.988590000	Link
CVE-2023-39143	0.940070000	0.991790000	Link
CVE-2023-38646	0.906240000	0.988640000	Link
CVE-2023-38205	0.954590000	0.994070000	Link
CVE-2023-38203	0.968820000	0.997260000	Link
CVE-2023-38146	0.905210000	0.988540000	Link
CVE-2023-38035	0.974190000	0.999400000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.963940000	0.995870000	Link
CVE-2023-3519	0.965360000	0.996280000	Link
CVE-2023-35082	0.967060000	0.996740000	Link
CVE-2023-35078	0.968330000	0.997130000	Link
CVE-2023-34993	0.971260000	0.998120000	Link
CVE-2023-34960	0.927460000	0.990380000	Link
CVE-2023-34634	0.927960000	0.990420000	Link
CVE-2023-34468	0.906650000	0.988660000	Link
CVE-2023-34362	0.969920000	0.997620000	Link
CVE-2023-34039	0.944490000	0.992390000	Link
CVE-2023-3368	0.933870000	0.991110000	Link
CVE-2023-33246	0.972790000	0.998690000	Link
CVE-2023-32315	0.973570000	0.999070000	Link
CVE-2023-30625	0.943100000	0.992160000	Link
CVE-2023-30013	0.962250000	0.995430000	Link
CVE-2023-29300	0.968380000	0.997150000	Link
CVE-2023-29298	0.943170000	0.992190000	Link
CVE-2023-28771	0.902140000	0.988370000	Link
CVE-2023-28343	0.948520000	0.993020000	Link
CVE-2023-28121	0.909760000	0.988860000	Link
CVE-2023-27524	0.970570000	0.997810000	Link
CVE-2023-27372	0.973020000	0.998800000	Link
CVE-2023-27350	0.969800000	0.997580000	Link
CVE-2023-26469	0.935230000	0.991240000	Link
CVE-2023-26360	0.962310000	0.995460000	Link
CVE-2023-26035	0.967100000	0.996750000	Link
CVE-2023-25717	0.956860000	0.994460000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.969960000	0.997630000	Link
CVE-2023-2479	0.963760000	0.995830000	Link
CVE-2023-24489	0.973310000	0.998950000	Link
CVE-2023-23752	0.954250000	0.994020000	Link
CVE-2023-23397	0.901800000	0.988350000	Link
CVE-2023-23333	0.964220000	0.995930000	Link
CVE-2023-22527	0.970550000	0.997810000	Link
CVE-2023-22518	0.965950000	0.996420000	Link
CVE-2023-22515	0.973330000	0.998960000	Link
CVE-2023-21839	0.956220000	0.994380000	Link
CVE-2023-21554	0.950840000	0.993380000	Link
CVE-2023-20887	0.970320000	0.997750000	Link
CVE-2023-1671	0.962480000	0.995500000	Link
CVE-2023-0669	0.969330000	0.997420000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 10 Jul 2024

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

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

- Link

—

Wed, 10 Jul 2024

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

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

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Microsoft .NET Framework: Mehrere Schwachstellen

Ein lokaler oder ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework und Microsoft Visual Studio 2022 ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und eine Denial-of-Service-Situation zu erzeugen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Microsoft 365 Apps, Microsoft Office, Microsoft Office 2016, Microsoft Office 2019, Microsoft Outlook 2016, Microsoft SharePoint und Microsoft SharePoint Server 2019 ausnutzen, um Informationen offenzulegen oder um beliebigen Code auszuführen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Microsoft SQL Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft SQL Server 2016, Microsoft SQL Server 2017, Microsoft SQL Server 2019 und Microsoft SQL Server 2022 ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Microsoft System Center: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Microsoft Defender ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen

Ein entfernter, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Azure, Microsoft Azure DevOps Server und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und Dateien zu manipulieren.

- Link

—

Wed, 10 Jul 2024

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

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

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Siemens JT2Go: Schwachstelle ermöglicht Codeausführung und DoS

Ein entfernter anonymer Angreifer kann eine Schwachstelle in Siemens JT2Go ausnutzen, um beliebigen Code auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Siemens TIA Portal: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter anonymer oder lokal privilegierter Angreifer kann mehrere Schwachstellen in Siemens TIA Portal ausnutzen, um beliebigen Code auszuführen.

- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Django: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Django ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 10 Jul 2024

[NEU] [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

—

Wed, 10 Jul 2024

[NEU] [hoch] lighttpd: Schwachstelle ermöglicht Denial of Service und Informationsoffenlegung

Ein entfernter anonymer Angreifer kann eine Schwachstelle in lighttpd ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.
- Link

—

Wed, 10 Jul 2024

[UPDATE] [hoch] Ghostscript: Mehrere Schwachstellen

Ein entfernter anonymer oder ein lokaler Angreifer kann mehrere Schwachstellen in Ghostscript ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.
- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Citrix Systems NetScaler Console, Agent und SVM: Mehrere Schwachstellen

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Citrix Systems NetScaler ausnutzen, um einen Denial of Service Angriff durchzuführen und vertrauliche Informationen offenzulegen.
- Link

—

Wed, 10 Jul 2024

[NEU] [hoch] Lenovo XClarity: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Lenovo XClarity ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.
- Link

—

Wed, 10 Jul 2024

[UPDATE] [hoch] Bluetooth Spezifikation: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Bluetooth Chipsätzen zahlreicher Hersteller ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Wed, 10 Jul 2024

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

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

—

Wed, 10 Jul 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libTIFF ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/10/2024	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2024-192-01)]	critical
7/10/2024	[Oracle Linux 9 : dotnet6.0 (ELSA-2024-4439)]	high
7/10/2024	[RHEL 8 : dotnet8.0 (RHSA-2024:4451)]	high
7/10/2024	[RHEL 9 : dotnet8.0 (RHSA-2024:4450)]	high
7/10/2024	[Juniper Junos OS Multiple Vulnerabilities (JSA82975)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA83011)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA82991)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA82989)]	high
7/10/2024	[Palo Alto Networks PAN-OS 10.1.x < 10.1.9 / 10.2.x < 10.2.4 Vulnerability]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA83023)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA83008)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA83000)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA75726)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA79101)]	high
7/10/2024	[Juniper Junos OS Vulnerability (JSA82982)]	high
7/10/2024	[FreeBSD : Django – multiple vulnerabilities (171afa61-3eba-11ef-a58f-080027836e8b)]	high
7/10/2024	[Oracle Linux 8 : dotnet6.0 (ELSA-2024-4438)]	high

Datum	Schwachstelle	Bewertung
7/10/2024	[Wireshark 4.0.x < 4.0.16 A Vulnerability]	high
7/10/2024	[Wireshark 4.0.x < 4.0.16 A Vulnerability (macOS)]	high
7/10/2024	[Wireshark 4.2.x < 4.2.6 A Vulnerability]	high
7/10/2024	[Wireshark 4.2.x < 4.2.6 A Vulnerability (macOS)]	high
7/10/2024	[Oracle Linux 9 : dotnet8.0 (ELSA-2024-4450)]	high
7/10/2024	[Oracle Linux 8 : dotnet8.0 (ELSA-2024-4451)]	high
7/10/2024	[Oracle Linux 9 : openssh (ELSA-2024-4457)]	high
7/10/2024	[AlmaLinux 9 : dotnet6.0 (ALSA-2024:4439)]	high
7/10/2024	[RHEL 8 : ghostscript (RHSA-2024:4462)]	high
7/10/2024	[RHEL 8 : python3 (RHSA-2024:4456)]	high
7/10/2024	[RHEL 9 : openssh (RHSA-2024:4457)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 10 Jul 2024

Microsoft SharePoint Remote Code Execution

This archive contains three proof of concepts exploit for multiple Microsoft SharePoint remote code execution vulnerabilities.

- Link

—

” “Tue, 09 Jul 2024

Ivanti EPM RecordGoodApp SQL Injection / Remote Code Execution

Ivanti Endpoint Manager (EPM) 2022 SU5 and prior versions are susceptible to an unauthenticated SQL injection vulnerability which can be leveraged to achieve unauthenticated remote code execution.

- Link

—

” “Mon, 08 Jul 2024

WordPress Poll 2.3.6 SQL Injection

WordPress Poll plugin version 2.3.6 suffers from a remote SQL injection vulnerability.
- Link

—

” “Mon, 08 Jul 2024

VMWare Aria Operations For Networks Command Injection

VMWare Aria Operations for Networks (vRealize Network Insight) is vulnerable to command injection when accepting user input through the Apache Thrift RPC interface. This is a proof of concept exploit.
- Link

—

” “Mon, 08 Jul 2024

Veeam Backup Enterprise Manager Authentication Bypass

Veeam Backup Enterprise Manager authentication bypass proof of concept exploit. Versions prior to 12.1.2.172 are vulnerable.
- Link

—

” “Mon, 08 Jul 2024

Veeam Recovery Orchestrator Authentication Bypass

Veeam Recovery Orchestrator authentication bypass proof of concept exploit.
- Link

—

” “Mon, 08 Jul 2024

Telerik Report Server Deserialization / Authentication Bypass

Telerik Report Server deserialization and authentication bypass exploit chain that makes use of the vulnerabilities noted in CVE-2024-4358 and CVE-2024-1800.
- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold WriteDatafile Unauthenticated Remote Code Execution

Progress WhatsUp Gold WriteDatafile unauthenticated remote code execution proof of concept exploit.
- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold GetFileWithoutZip Unauthenticated Remote Code Execution

Progress WhatsUp Gold GetFileWithoutZip unauthenticated remote code execution proof of concept exploit.
- Link

—

” “Mon, 08 Jul 2024

Progress WhatsUp Gold SetAdminPassword Privilege Escalation

Progress WhatsUp Gold SetAdminPassword local privilege escalation proof of concept exploit.

- Link

—

” “Mon, 08 Jul 2024

ResidenceCMS 2.10.1 Cross Site Scripting

ResidenceCMS versions 2.10.1 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jul 2024

PMS 2024 1.0 SQL Injection

PMS 2024 version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Jul 2024

Simple Online Banking System 1.0 SQL Injection

Simple Online Banking System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 08 Jul 2024

Microsoft Office 365 Remote Code Execution

Microsoft Office 365 appears susceptible to macro code execution that can result in remote code execution.

- Link

—

” “Fri, 05 Jul 2024

WordPress Video Gallery - YouTube Gallery And Vimeo Gallery 2.3.6 SQL Injection

WordPress Video Gallery - YouTube Gallery And Vimeo Gallery version 2.3.6 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 05 Jul 2024

Cinema Booking System 1.0 SQL Injection / Cross Site Request Forgery

Cinema Booking System version 1.0 suffers from remote SQL injection and cross site request forgery vulnerabilities.

- Link

—

” “Thu, 04 Jul 2024

Helmholz Industrial Router REX100 / MBConnectline mbNET.mini 2.2.11 Command Injection

Helmholz Industrial Router REX100 and MBConnectline mbNET.mini versions 2.2.11 and below suffer from a command injection vulnerability.

- Link

—

” “Thu, 04 Jul 2024

Toshiba Multi-Function Printers 40 Vulnerabilities

103 models of Toshiba Multi-Function Printers (MFP) are vulnerable to 40 different vulnerabilities including remote code execution, local privilege escalation, xml injection, and more.

- Link

—

” “Thu, 04 Jul 2024

Zyxel parse_config.py Command Injection

This Metasploit module exploits vulnerabilities in multiple Zyxel devices including the VPN, USG and APT series. The affected firmware versions depend on the device module, see this module’s documentation for more details.

- Link

—

” “Thu, 04 Jul 2024

Sharp Multi-Function Printer 18 Vulnerabilities

308 different models of Sharp Multi-Function Printers (MFP) are vulnerable to 18 different vulnerabilities including remote code execution, local file inclusion, credential disclosure, and more.

- Link

—

” “Thu, 04 Jul 2024

SoftMaker Office / FreeOffice Local Privilege Escalation

SoftMaker Office and FreeOffice suffer from a local privilege escalation vulnerability via the MSI installer. Vulnerable versions include SoftMaker Office 2024 / NX before revision 1214, FreeOffice 2021 Revision 1068, and FreeOffice 2024 before revision 1215.

- Link

—

” “Thu, 04 Jul 2024

WordPress Photo Gallery 1.8.26 Cross Site Scripting

WordPress Photo Gallery plugin version 1.8.26 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 04 Jul 2024

Siemens CP-8000 / CP-8021 / CP8-022 / CP-8031 / CP-8050 / SICORE Buffer Overread / Escalation

Siemens CP-8000, CP-8021, CP8-022, CP-8031, CP-8050, and SICORE products suffer from buffer overread, privilege escalation, and unsafe storage vulnerabilities.

- Link

—

” “Wed, 03 Jul 2024

Deep Sea Electronics DSE855 Remote Authentication Bypass

Deep Sea Electronics DSE855 is vulnerable to configuration disclosure when direct object reference is made to the Backup.bin file using an HTTP GET request. This will enable an attacker to disclose sensitive information and help her in authentication bypass, privilege escalation, and full system access.

- Link

—

” “Tue, 02 Jul 2024

WordPress FooGallery 2.4.16 Cross Site Scripting

WordPress FooGallery plugin version 2.4.16 suffers from a persistent cross site scripting 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: (Jul)

Datum	Opfer	Land	Information
2024-07-09	Clay County Courthouse	[USA]	Link
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	Link
2024-07-04	La Ville d'Ans	[BEL]	Link
2024-07-03	E.S.E. Salud Yopal	[COL]	Link
2024-07-03	Florida Department of Health	[USA]	Link
2024-07-02	Hong Kong Institute of Architects	[HKG]	Link
2024-07-02	Apex	[USA]	Link
2024-07-01	Hiap Seng Industries	[SGP]	Link
2024-07-01	Monroe County government	[USA]	Link

7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-11	[Texas Electric Cooperatives]	play	Link
2024-07-11	[The 21st Century Energy Group]	play	Link
2024-07-11	[T P C I]	play	Link
2024-07-10	[City of Cedar Falls]	blacksuit	Link
2024-07-10	[P448]	akira	Link
2024-07-10	[Beowulfchain]	vanirgroup	Link
2024-07-10	[Qinao]	vanirgroup	Link
2024-07-10	[Athlon]	vanirgroup	Link
2024-07-10	[Usina Alta Mogiana S/A]	akira	Link
2024-07-09	[Inland Audio Visual]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-09	[Indika Energy]	hunters	Link
2024-07-08	[Excelsior Orthopaedics]	monti	Link
2024-07-09	[Heidmar]	akira	Link
2024-07-03	[REPLIGEN]	incransom	Link
2024-07-08	[Raffmetal Spa]	dragonforce	Link
2024-07-08	[Allied Industrial Group]	akira	Link
2024-07-08	[Esedra]	akira	Link
2024-07-08	[Federated Co-operatives]	akira	Link
2024-07-02	[Guhring USA]	incransom	Link
2024-07-06	[noab.nl]	lockbit3	Link
2024-07-07	[Strauss Brands]	medusa	Link
2024-07-07	[Harry Perkins Institute of medical research]	medusa	Link
2024-07-07	[Viasat]	medusa	Link
2024-07-07	[Olympus Group]	medusa	Link
2024-07-07	[MYC Media]	rhysida	Link
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	Link
2024-07-03	[baiminstitute.org]	ransomhub	Link
2024-07-05	[The Wacks Law Group]	qilin	Link
2024-07-05	[pomalca.com.pe]	qilin	Link
2024-07-05	[Center for Human Capital Innovation (centerforhci.org)]	incransom	Link
2024-07-05	[waupacacounty-wi.gov]	incransom	Link
2024-07-05	[waupaca.wi.us]	incransom	Link
2024-07-04	[ws-stahl.eu]	lockbit3	Link
2024-07-04	[homelandvinyl.com]	lockbit3	Link
2024-07-04	[eicher.in]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-05	[National Health Laboratory Services]	blacksuit	Link
2024-07-04	[Un Museau]	spacebears	Link
2024-07-03	[Haylem]	spacebears	Link
2024-07-04	[Elyria Foundry]	play	Link
2024-07-04	[Texas Recycling]	play	Link
2024-07-04	[INDA's]	play	Link
2024-07-04	[Innerspec Technologies]	play	Link
2024-07-04	[Prairie Athletic Club]	play	Link
2024-07-04	[Fareri Associates]	play	Link
2024-07-04	[Island Transportation Corp.]	bianlian	Link
2024-07-04	[Legend Properties, Inc.]	bianlian	Link
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	Link
2024-07-03	[hcri.edu]	ransomhub	Link
2024-07-04	[Coquitlam Concrete]	hunters	Link
2024-07-04	[Multisuns Communication]	hunters	Link
2024-07-04	[gerard-perrier.com]	embargo	Link
2024-07-04	[Abileneisd.org]	cloak	Link
2024-07-03	[sequelglobal.com]	darkvault	Link
2024-07-03	[Explomin]	akira	Link
2024-07-03	[Alimac]	akira	Link
2024-07-03	[badel1862.hr]	blackout	Link
2024-07-03	[ramservices.com]	underground	Link
2024-07-03	[foremedia.net]	darkvault	Link
2024-07-03	[www.swcs-inc.com]	ransomhub	Link
2024-07-03	[valleylandtitleco.com]	donutleaks	Link
2024-07-02	[merrymanhouse.org]	lockbit3	Link
2024-07-02	[fairfieldmemorial.org]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-02	[www.daesangamerica.com]	ransomhub	Link
2024-07-02	[P1 Technologies]	akira	Link
2024-07-02	[Conexus Medstaff]	akira	Link
2024-07-02	[Salton]	akira	Link
2024-07-01	[www.sfmedical.de]	ransomhub	Link
2024-07-02	[WheelerShip]	hunters	Link
2024-07-02	[Grand Rapids Gravel]	dragonforce	Link
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	Link
2024-07-02	[Elite Fitness]	dragonforce	Link
2024-07-02	[Gray & Adams]	dragonforce	Link
2024-07-02	[Vermont Panurgy]	dragonforce	Link
2024-07-01	[floridahealth.gov]	ransomhub	Link
2024-07-01	[www.nttdata.ro]	ransomhub	Link
2024-07-01	[Super Gardens]	dragonforce	Link
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinusa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	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.