Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240912

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

Ivanti: Updates gegen kritische Lecks im Endpoint Manager und weiteren Produkten
Ivanti bessert Schwachstellen in Endpoint Manager, Workspace Control und Cloud Service Appliance aus. Eine Lücke in EPM erreicht die Höchstwertung CVSS 10.
- Link

—

ownCloud: Update stopft teils hochriskante Sicherheitslücken
Das ownCloud-Projekt warnt vor Sicherheitslücken in der Kollaborationssoftware. Angreifer können etwa Zugriff auf Zugangsdaten erlangen.
- Link

—

Citrix Workspace App für Windows ermöglicht Rechteausweitung
In der Citrix Workspace App für Windows klaffen zwei Sicherheitslücken. Angreifer können dadurch ihre Rechte im System ausweiten.
- Link

—

Adobe-Patchday: Kritische Lücken in mehreren Produkten
Adobe stopft am Patchday mehrere kritische Sicherheitslecks. Updates gibt es für acht Produkte des Herstellers.
- Link

—

Patchday Microsoft: Angreifer attackieren vier Lücken in Windows & Co.
Microsoft hat Schwachstellen in unter anderem Azure, SharePoint und Windows geschlossen. Einige Lücken gelten als kritisch.
- Link

—

CISA warnt: Acht Jahre alte Lücke in ImageMagick und weitere angegriffen
Die CISA warnt, dass in ImageMagick eine acht Jahre alte Sicherheitslücke angegriffen wird. Ebenso eine sieben Jahre alte Lücke in Linux.
- Link

—

SAP-Patchday: 16 Sicherheitsmitteilungen zu diversen Produkten
Am September-Patchday hat SAP 16 neue Sicherheitsmitteilungen herausgegeben. Sie behandeln Lücken, die als mittleres oder niedriges Risiko gelten.
- Link

—

Loadbalancer: Angreifer können LoadMaster kompromittieren

Es sind wichtige Sicherheitspatches für LoadMaster und MultiTenant Hypervisor von Progress Kemp erschienen.

- Link

—

Schadcode-Lücken gefährden Visualiserungsplattform Kibana

Ein Sicherheitsupdate schließt zwei kritische Sicherheitslücken in Kibana.

- Link

—

Jetzt patchen! Angreifer attackieren Firewalls von Sonicwall

Mittlerweile ist klar, dass eine Schwachstelle nicht nur SonicOS, sondern auch die SSLVPN-Funktion betrifft. Sicherheitsupdates sind verfügbar.

- 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	0.957050000	0.994780000	Link
CVE-2023-6895	0.921160000	0.990210000	Link
CVE-2023-6553	0.937150000	0.991830000	Link
CVE-2023-6019	0.918710000	0.989950000	Link
CVE-2023-5360	0.902780000	0.988900000	Link
CVE-2023-52251	0.946410000	0.992950000	Link
CVE-2023-4966	0.970840000	0.998130000	Link
CVE-2023-49103	0.949680000	0.993510000	Link
CVE-2023-48795	0.965330000	0.996470000	Link
CVE-2023-47246	0.956040000	0.994610000	Link
CVE-2023-46805	0.950230000	0.993610000	Link
CVE-2023-46747	0.972260000	0.998650000	Link
CVE-2023-46604	0.968800000	0.997440000	Link
CVE-2023-4542	0.948590000	0.993320000	Link
CVE-2023-43208	0.973970000	0.999390000	Link
CVE-2023-43177	0.961750000	0.995590000	Link
CVE-2023-42793	0.971190000	0.998300000	Link
CVE-2023-41265	0.907590000	0.989210000	Link
CVE-2023-39143	0.936490000	0.991770000	Link
CVE-2023-38205	0.950330000	0.993620000	Link
CVE-2023-38203	0.965830000	0.996620000	Link
CVE-2023-38146	0.920720000	0.990150000	Link
CVE-2023-38035	0.974690000	0.999720000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996880000	Link
CVE-2023-3519	0.965910000	0.996640000	Link
CVE-2023-35082	0.967460000	0.997070000	Link
CVE-2023-35078	0.970930000	0.998180000	Link
CVE-2023-34993	0.973450000	0.999170000	Link
CVE-2023-34960	0.921610000	0.990280000	Link
CVE-2023-34634	0.923140000	0.990400000	Link
CVE-2023-34362	0.970450000	0.997970000	Link
CVE-2023-34039	0.947070000	0.993060000	Link
CVE-2023-3368	0.939780000	0.992150000	Link
CVE-2023-33246	0.967830000	0.997170000	Link
CVE-2023-32315	0.970220000	0.997880000	Link
CVE-2023-30625	0.953610000	0.994190000	Link
CVE-2023-30013	0.965950000	0.996660000	Link
CVE-2023-29300	0.969240000	0.997580000	Link
CVE-2023-29298	0.970810000	0.998110000	Link
CVE-2023-28432	0.907350000	0.989190000	Link
CVE-2023-28343	0.933130000	0.991470000	Link
CVE-2023-28121	0.925430000	0.990640000	Link
CVE-2023-27524	0.970600000	0.998020000	Link
CVE-2023-27372	0.973930000	0.999360000	Link
CVE-2023-27350	0.968480000	0.997340000	Link
CVE-2023-26469	0.953890000	0.994240000	Link
CVE-2023-26360	0.964390000	0.996170000	Link
CVE-2023-26035	0.968440000	0.997320000	Link
CVE-2023-25717	0.954660000	0.994370000	Link
CVE-2023-25194	0.966980000	0.996940000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996070000	Link
CVE-2023-24489	0.973820000	0.999320000	Link
CVE-2023-23752	0.951460000	0.993790000	Link
CVE-2023-23333	0.961070000	0.995450000	Link
CVE-2023-22527	0.970940000	0.998200000	Link
CVE-2023-22518	0.961800000	0.995590000	Link
CVE-2023-22515	0.972760000	0.998900000	Link
CVE-2023-21839	0.951270000	0.993730000	Link
CVE-2023-21554	0.955880000	0.994580000	Link
CVE-2023-20887	0.970840000	0.998130000	Link
CVE-2023-1671	0.962690000	0.995760000	Link
CVE-2023-0669	0.971330000	0.998380000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 11 Sep 2024

[UPDATE] [hoch] SonicWall SonicOS: Schwachstelle ermöglicht Offenlegung von Informationen und Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in SonicWall SonicOS ausnutzen, um Informationen offenzulegen und um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 11 Sep 2024

[NEU] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in mehreren Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmaßnahmen zu umgehen und Plattform- und Service-Spoofing durchzuführen.

- Link

—

Wed, 11 Sep 2024

[NEU] [kritisch] Ivanti Endpoint Manager: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ivanti Endpoint Manager ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, erweiterte Rechte zu erlangen und vertrauliche Informationen preiszugeben.

- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] Microsoft Dynamics 365: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Dynamics 365 ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen oder einen Spoofing-Angriff durchzuführen.

- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft 365 Apps, Microsoft Excel 2016, Microsoft Office, Microsoft Office 2019, Microsoft Office Online Server, Microsoft Outlook, Microsoft Publisher 2016, Microsoft SharePoint, Microsoft SharePoint Server 2019 und Microsoft Visio 2016 ausnutzen, um seine Privilegien zu erhöhen, Sicherheitsmaßnahmen zu umgehen und beliebigen Code auszuführen.

- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure Komponenten ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- Link

—

Wed, 11 Sep 2024

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

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Microsoft SQL Server ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Wed, 11 Sep 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

—

Wed, 11 Sep 2024

[NEU] [hoch] Lenovo XClarity: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Lenovo XClarity ausnutzen, um seine Privilegien zu erhöhen, beliebige Befehle auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] Adobe Creative Cloud Applikationen: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Adobe Creative Cloud ausnutzen, um beliebigen Programmcode auszuführen und einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] Lenovo XClarity Administrator (LXCA): Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein Angreifer kann mehrere Schwachstellen in Lenovo XClarity ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen ausnutzen oder nicht näher beschriebene Auswirkungen zu erzielen.
- Link

—

Wed, 11 Sep 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.
- Link

—

Wed, 11 Sep 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 11 Sep 2024

[UPDATE] [hoch] Red Hat JBoss A-MQ: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss A-MQ ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 11 Sep 2024

[UPDATE] [hoch] Microsoft SQL Server und Visual Studio: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft SQL Server und Microsoft Visual Studio ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 11 Sep 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

—

Wed, 11 Sep 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Wed, 11 Sep 2024

[UPDATE] [kritisch] FRRouting Project FRRouting: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Zustand zu erzeugen und potenziell beliebigen Programmcode auszuführen.

- Link

—

Wed, 11 Sep 2024

[NEU] [hoch] IBM InfoSphere Information Server: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in IBM InfoSphere Information Server ausnutzen, um Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen Denial of Service zu verursachen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/11/2024	[WordPress Plugin 'LiteSpeed Cache' < 6.5.0.1. Unauthenticated Account Takeover]	critical
9/11/2024	[LangChain Experimental Python Library <= 0.0.14 (CVE-2023-44467)]	critical
9/11/2024	[AlmaLinux 9 : emacs (ALSA-2024:6510)]	critical
9/11/2024	[RHEL 7 : httpd (RHSA-2024:6584)]	critical
9/11/2024	[RHEL 9 : git (RHSA-2024:6610)]	critical
9/11/2024	[Oracle Linux 8 : Unbreakable Enterprise kernel (ELSA-2024-12610)]	critical
9/11/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel-container (ELSA-2024-12612)]	critical
9/11/2024	[openSUSE 15 Security Update : python-Django (SUSE-SU-2024:3187-1)]	high
9/11/2024	[SUSE SLES12 Security Update : java-1_8_0-ibm (SUSE-SU-2024:3183-1)]	high
9/11/2024	[SUSE SLES12 Security Update : kernel (SUSE-SU-2024:3189-1)]	high

Datum	Schwachstelle	Bewertung
9/11/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:3195-1)]	high
9/11/2024	[SUSE SLES15 Security Update : buildah (SUSE-SU-2024:3186-1)]	high
9/11/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:3190-1)]	high
9/11/2024	[SUSE SLES12 Security Update : postgresql16 (SUSE-SU-2024:3192-1)]	high
9/11/2024	[SUSE SLES12 Security Update : go1.22 (SUSE-SU-2024:3196-1)]	high
9/11/2024	[FreeBSD : Intel CPUs – multiple vulnerabilities (d5026193-6fa2-11ef-99bc-1c697a616631)]	high
9/11/2024	[Photon OS 4.0: Linux PHSA-2024-4.0-0687]	high
9/11/2024	[Photon OS 5.0: Linux PHSA-2024-5.0-0370]	high
9/11/2024	[SUSE SLES12 Security Update : go1.23 (SUSE-SU-2024:3197-1)]	high
9/11/2024	[SUSE SLES12 Security Update : containerd (SUSE-SU-2024:3188-1)]	high
9/11/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:3194-1)]	high
9/11/2024	[SUSE SLES12 Security Update : postgresql16 (SUSE-SU-2024:3191-1)]	high
9/11/2024	[WordPress Plugin ‘LiteSpeed Cache’ < 5.7.0.1 Stored XSS]	high
9/11/2024	[Microsoft Power Automate For Desktop Remote Code Execution (CVE-2024-43479)]	high
9/11/2024	[Security Updates for Microsoft Dynamics 365 Business Central (September 2024)]	high
9/11/2024	[Security Updates for Microsoft Dynamics 365 (on-premises) (September 2024)]	high
9/11/2024	[LangChain Python Library < 0.0.317 (CVE-2023-46229)]	high

Datum	Schwachstelle	Bewertung
9/11/2024	[Golang < 1.22.7, 1.23.x < 1.23.1 Multiple Vulnerabilities]	high
9/11/2024	[Palo Alto Networks PAN-OS 11.2.x < 11.2.3 Vulnerability]	high
9/11/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-6999-1)]	high
9/11/2024	[Debian dsa-5768 : chromium - security update]	high
9/11/2024	[RHEL 9 : fence-agents (RHSA-2024:6611)]	high
9/11/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.14.36 (RHSA-2024:6412)]	high
9/11/2024	[RHEL 9 : fence-agents (RHSA-2024:6612)]	high
9/11/2024	[Ubuntu 14.04 LTS : LibTIFF vulnerability (USN-6997-2)]	high
9/11/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2024-12611)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 11 Sep 2024

VICIdial 2.14-917a Remote Code Execution

An attacker with authenticated access to VICIdial version 2.14-917a as an agent can execute arbitrary shell commands as the root user. This attack can be chained with CVE-2024-8503 to execute arbitrary shell commands starting from an unauthenticated perspective.

- Link

—

” “Wed, 11 Sep 2024

VICIdial 2.14-917a SQL Injection

An unauthenticated attacker can leverage a time-based SQL injection vulnerability in VICIdial version 2.14-917a to enumerate database records. By default, VICIdial stores plaintext credentials within the database.

- Link

—

” “Wed, 11 Sep 2024

Queuing Simple Chatbot 1.0 Shell Upload

Queuing Simple Chatbot version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Wed, 11 Sep 2024

Profiling System 1.0 Shell Upload

Profiling System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Wed, 11 Sep 2024

Passion Responsive Blogging 1.0 Cross Site Scripting

Passion Responsive Blogging version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 11 Sep 2024

Online Survey System 1.0 Cross Site Scripting / Remote File Inclusion

Online Survey System version 1.0 suffers from cross site scripting and remote file inclusion vulnerabilities.

- Link

—

” “Wed, 11 Sep 2024

Online Birth Certificate System 1.0 Insecure Settings

Online Birth Certificate System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 11 Sep 2024

Medical Card Generations System 1.0 Insecure Settings

Medical Card Generations System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 11 Sep 2024

Emergency Ambulance Hiring Portal 1.0 WYSIWYG Code Injection

Emergency Ambulance Hiring Portal version 1.0 suffer from a WYSIWYG code injection vulnerability.

- Link

—

” “Wed, 11 Sep 2024

Printable Staff ID Card Creator System 1.0 Insecure Direct Object Reference

Printable Staff ID Card Creator System version 1.0 suffers from an insecure direct object reference

vulnerability.

- Link

—

” “Tue, 10 Sep 2024

GitHub sqlpad/sqlpad Template Injection / Remote Code Execution

Proof of concept automation code to exploit a template injection vulnerability in GitHub repository sqlpad/sqlpad version prior to 6.10.1 that can result in remote code execution.

- Link

—

” “Tue, 10 Sep 2024

Spring Cloud Data Flow Remote Code Execution

Proof of concept exploit for Spring Cloud Data Flow versions prior to 2.11.4 that achieves remote code execution through a malicious upload.

- Link

—

” “Tue, 10 Sep 2024

PowerVR DEVMEMXINT_RESERVATION::ppsPMR Use-After-Free

The array ppsPMR in DEVMEMXINT_RESERVATION holds references to PMR structures (using PMRRefPMR2()), intending to prevent the PMRs’ physical memory from being released. However, PMRs with PVRSRV_MEMALLOCFLAG_NO_OSPAGES_ON_ALLOC (which for OSMem PMRs internally translates to FLAG_ONDEMAND) can release their backing physical pages while references to the PMR still exist; PMRLockSysPhysAddresses() must be used to prevent a PMR’s backing pages from disappearing, like in DevmemIntMapPMR2(). Therefore, it is currently possible to free a PMR’s backing pages while the PMR is mapped into a DEVMEMXINT_RESERVATION, leading to physical page use-after-free.

- Link

—

” “Tue, 10 Sep 2024

Prison Management System 1.0 Add Administrator

Prison Management System version 1.0 suffers from an add administrator vulnerability.

- Link

—

” “Tue, 10 Sep 2024

Online Survey System 1.0 Remote File Inclusion

Online Survey System version 1.0 suffers from a remote file inclusion vulnerability.

- Link

—

” “Tue, 10 Sep 2024

Online Student Grading System 1.0 SQL Injection

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

- Link

—

” “Tue, 10 Sep 2024

Online Marriage Registration System 1.0 Shell Upload

Online Marriage Registration System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 10 Sep 2024

Dairy Farm Shop Management System 1.2 SQL Injection / Code Execution

Dairy Farm Shop Management System version 1.2 suffers from a remote SQL injection vulnerability that allows for a backdoor to be inserted for code execution.

- Link

—

” “Tue, 10 Sep 2024

Beauty Parlour Management System 1.0 SQL Injection / Code Execution

Beauty Parlour Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for a backdoor to be inserted for code execution.

- Link

—

” “Tue, 10 Sep 2024

Apartment Visitor Management System 1.0 SQL Injection / Code Execution

Apartment Visitor Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for a backdoor to be inserted for code execution.

- Link

—

” “Tue, 10 Sep 2024

Passion Responsive Blogging 1.0 SQL Injection

Passion Responsive Blogging version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 09 Sep 2024

Microsoft Windows DWM Core Library Privilege Escalation

Proof of concept code for the Microsoft Windows DWM Core library elevation of privilege vulnerability. The researcher shows how they reversed the patch, how the heap overflow is produced, and overall gives a complete walk through of their process.

- Link

—

” “Mon, 09 Sep 2024

Breaking Oracle Database VPD Through DDL Permissions In 19c

By having specific DDL permissions set in Oracle 19c, you can bypass access restrictions normally in place for VPD (virtual private database).

- Link

—

” “Mon, 09 Sep 2024

PPDB 2.4-update 6118-1 SQL Injection

PPDB version 2.4-update 6118-1 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Mon, 09 Sep 2024

POMS 1.0 Insecure Settings

POMS version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 11 Sep 2024

ZDI-24-1222: Ivanti Workspace Control RES Exposed Dangerous Method Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1221: Ivanti Endpoint Manager LoadMotherboardTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1220: Ivanti Endpoint Manager LoadSlotsTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1219: Ivanti Endpoint Manager loadModuleTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1218: Ivanti Endpoint Manager updateAssetInfo SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1217: Ivanti Endpoint Manager loadSystemInfo SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1216: Ivanti Endpoint Manager GetSQLStatement SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1215: Ivanti Endpoint Manager loadKeyboardTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1214: Ivanti Endpoint Manager GetVulnerabilitiesDataTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1213: Ivanti Endpoint Manager loadMouseTable SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1212: Ivanti Endpoint Manager ImportXml XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1211: Ivanti Endpoint Manager WasPreviouslyMapped SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1210: Microsoft Windows Drag and Drop SmartScreen Bypass Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1209: Microsoft Windows Defender SmartScreen Bypass Vulnerability

- Link

—

” “Wed, 11 Sep 2024

ZDI-24-1208: (0Day) Visteon Infotainment System DeviceManager iAP Serial Number SQL Injection Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1207: Microsoft Windows Internet Explorer File Extension Spoofing Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1206: Microsoft SharePoint SPAutoSerializingObject Deserialization of Untrusted Data Denial-of-Service Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1205: Microsoft Windows BeginPaint Pen Use-After-Free Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1204: Microsoft SharePoint SPThemes Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1203: Adobe Photoshop JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1202: Adobe After Effects AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1201: Adobe Premiere Pro AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1200: Adobe Media Encoder AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1199: Adobe After Effects AVI File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1198: Adobe Premiere Pro AVI File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

” “Tue, 10 Sep 2024

ZDI-24-1197: Adobe Audition AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 09 Sep 2024

ZDI-24-1196: Adobe Acrobat Reader DC Doc Object Use-After-Free Information Disclosure Vul-

nerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection.

Zum Youtube Video

6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-09	Université de Gênes	[ITA]	Link
2024-09-09	University and College Union (UCU)	[GBR]	Link
2024-09-08	Highline Public Schools	[USA]	Link
2024-09-08	Groupe Bayard	[FRA]	Link
2024-09-06	Superior Tribunal de Justiça (STJ)	[BRA]	Link
2024-09-05	Air-e	[COL]	Link
2024-09-05	Charles Darwin School	[GBR]	Link
2024-09-05	Elektroskandia	[SWE]	Link
2024-09-04	Tewkesbury Borough Council	[GBR]	Link
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	Link
2024-09-02	Transport for London (TfL)	[GBR]	Link
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	Link
2024-09-01	Wertachkliniken	[DEU]	Link

7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-10	[allamericanpoly.com]	ransomhub	Link
2024-09-11	[Charles Darwin School]	blacksuit	Link
2024-09-11	[S. Walter Packaging]	fog	Link
2024-09-11	[Clatronic International GmbH]	fog	Link
2024-09-11	[Advanced Physician Management Services LLC]	meow	Link
2024-09-11	[Arville]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-11	[ICBC London]	hunters	Link
2024-09-11	[Ladov Law Firm]	bianlian	Link
2024-09-10	[Regent Care Center]	incransom	Link
2024-09-10	[www.vinatiorganics.com]	ransomhub	Link
2024-09-10	[Evans Distribution Systems]	play	Link
2024-09-10	[Weldco-Beales Manufacturing]	play	Link
2024-09-10	[PIGGLY WIGGLY ALABAMA DISTRIBUTING]	play	Link
2024-09-10	[Elgin Separation Solutions]	play	Link
2024-09-10	[Bel-Air Bay Club]	play	Link
2024-09-10	[Joe Swartz Electric]	play	Link
2024-09-10	[Virginia Dare Extract Co.]	play	Link
2024-09-10	[Southeast Cooler]	play	Link
2024-09-10	[IDF and Mossad agents]	meow	Link
2024-09-10	[rupicard.com]	killsec	Link
2024-09-10	[Vickers Engineering]	akira	Link
2024-09-09	[Controlled Power]	dragonforce	Link
2024-09-09	[Arc-Com]	dragonforce	Link
2024-09-10	[HDI]	bianlian	Link
2024-09-10	[Myelec Electrical]	meow	Link
2024-09-10	[Kadokawa Co Jp]	blacksuit	Link
2024-09-10	[Qeco/coeq]	rhysida	Link
2024-09-10	[E-Z Pack Holdings LLC]	incransom	Link
2024-09-10	[Bank Rakyat]	hunters	Link
2024-09-06	[americagraphics.com]	ransomhub	Link
2024-09-09	[Pennsylvania State Education Association]	rhysida	Link
2024-09-09	[Anniversary Holding]	bianlian	Link
2024-09-09	[Battle Lumber Co.]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-09	[www.unige.it]	ransomhub	Link
2024-09-09	[Appellation vins fins]	ransomhub	Link
2024-09-09	[www.dpe.go.th]	ransomhub	Link
2024-09-09	[www.bsg.com.au]	ransomhub	Link
2024-09-09	[schynsassurances.be]	killsec	Link
2024-09-09	[pv.be]	killsec	Link
2024-09-09	[Smart Source, Inc.]	bianlian	Link
2024-09-08	[CAM Tyre Trade Systems & Solutions]	qilin	Link
2024-09-09	[▒▒▒▒▒▒▒▒]	cicada3301	Link
2024-09-08	[Stratford School Academy]	rhysida	Link
2024-09-07	[cardiovirginia.com]	ransomhub	Link
2024-09-07	[Prosolit]	medusa	Link
2024-09-07	[Grupo Cortefiel]	medusa	Link
2024-09-07	[Nocciole Marchisio]	meow	Link
2024-09-07	[Elsoms Seeds]	meow	Link
2024-09-07	[Millsboro Animal Hospital]	qilin	Link
2024-09-05	[briedis.lt]	ransomhub	Link
2024-09-06	[America Voice]	medusa	Link
2024-09-06	[CK Associates]	bianlian	Link
2024-09-06	[Keya Accounting and Tax Services LLC]	bianlian	Link
2024-09-06	[ctelift.com]	madliberator	Link
2024-09-06	[SESAM Informatics]	hunters	Link
2024-09-06	[riomarineinc.com]	cactus	Link
2024-09-06	[champeau.com]	cactus	Link
2024-09-05	[cda.be]	killsec	Link
2024-09-05	[belfius.be]	killsec	Link
2024-09-05	[dvv.be]	killsec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-05	[Custom Security Systems]	hunters	Link
2024-09-05	[Inglenorth.co.uk]	ransomhub	Link
2024-09-05	[cps-k12.org]	ransomhub	Link
2024-09-05	[inorde.com]	ransomhub	Link
2024-09-05	[tri-tech.us]	ransomhub	Link
2024-09-05	[PhD Services]	dragonforce	Link
2024-09-05	[kawasaki.eu]	ransomhub	Link
2024-09-05	[phdservices.net]	ransomhub	Link
2024-09-05	[cbt-gmbh.de]	ransomhub	Link
2024-09-05	[www.towellengineering.net]	ransomhub	Link
2024-09-04	[rhp.com.br]	lockbit3	Link
2024-09-05	[Baird Mandalas Brockstedt LLC]	akira	Link
2024-09-05	[Imetame]	akira	Link
2024-09-05	[SWISS CZ]	akira	Link
2024-09-05	[Cellular Plus]	akira	Link
2024-09-05	[Arch Street Capital Advisors]	qilin	Link
2024-09-04	[Hospital Episcopal San Lucas]	medusa	Link
2024-09-05	[www.parknfly.ca]	ransomhub	Link
2024-09-05	[Western Supplies, Inc]	bianlian	Link
2024-09-04	[Farmers' Rice Cooperative]	play	Link
2024-09-04	[Bakersfield]	play	Link
2024-09-04	[Crain Group]	play	Link
2024-09-04	[Parrish]	blacksuit	Link
2024-09-04	[Seirus Innovation]	play	Link
2024-09-04	[www.galgorm.com]	ransomhub	Link
2024-09-04	[www.pcipa.com]	ransomhub	Link
2024-09-04	[OSDA Contract Services]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-09-04	[ych.com]	madliberator	Link
2024-09-04	[www.bennettcurrie.co.nz]	ransomhub	Link
2024-09-03	[idom.com]	lynx	Link
2024-09-04	[plannedparenthood.org]	ransomhub	Link
2024-09-04	[Sunrise Erectors]	hunters	Link
2024-09-03	[gardenhomesmanagement.com]	ransomhub	Link
2024-09-03	[simson-maxwell.com]	cactus	Link
2024-09-03	[balboabayresort.com]	cactus	Link
2024-09-03	[flodraulic.com]	cactus	Link
2024-09-03	[mcphillips.co.uk]	cactus	Link
2024-09-03	[rangeramerican.com]	cactus	Link
2024-09-02	[Kingsport Imaging Systems]	medusa	Link
2024-09-02	[www.amberbev.com]	ransomhub	Link
2024-09-02	[Removal.AI]	ransomhub	Link
2024-09-02	[Project Hospitality]	rhysida	Link
2024-09-02	[Shomof Group]	medusa	Link
2024-09-02	[www.sanyo-av.com]	ransomhub	Link
2024-09-01	[Quálitas México]	hunters	Link
2024-09-01	[welland]	trinity	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.