Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240109

Inhaltsverzeichnis

1 Editorial **2**

2 Security-News **3**
2.1 Heise - Security-Alert . . . 3

3 Sicherheitslücken **4**
3.1 EPSS . . . 4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . 5
3.2 BSI - Warn- und Informationsdienst (WID) . . . 6
3.3 Sicherheitslücken Meldungen von Tenable . . . 10

4 Aktiv ausgenutzte Sicherheitslücken **11**
4.1 Exploits der letzten 5 Tage . . . 11
4.2 0-Days der letzten 5 Tage . . . 15

5 Die Hacks der Woche **16**
5.0.1 Ihr habt WAS in eure Züge programmiert!? . . . 16

6 Cyberangriffe: (Jan) **17**

7 Ransomware-Erpressungen: (Jan) **17**

8 Quellen **18**
8.1 Quellenverzeichnis . . . 18

9 Impressum **20**

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

Jetzt patchen! Attacken auf Messaging-Plattform Apache RocketMQ

Angreifer scannen derzeit vermehrt nach verwundbaren RocketMQ-Servern. Sicherheitsupdates stehen bereit.

- Link

—

IBM warnt vor Sicherheitslücke in Db2

IBM warnt vor einer Sicherheitslücke in Db2. Angreifer können dadurch ihre Rechte in Windows-Systemen ausweiten. Updates stehen bereit.

- Link

—

Sicherheitsupdates: Schadcode- und DoS-Attacken auf Qnap NAS möglich

Angreifer können Netzwerkspeicher von Qnap ins Visier nehmen. Sicherheitspatches schaffen Abhilfe.

- Link

—

Kritische Schadcode-Lücke gefährdet Ivanti Endpoint Manager

Unter bestimmten Voraussetzungen können Angreifer Schadcode auf Ivanti-EPM-Servern ausführen.

- Link

—

Netzwerkanalysetool Wireshark gegen mögliche Attacken abgesichert

Die Wireshark-Entwickler haben in aktuellen Versionen mehrere Sicherheitslücken geschlossen.

- Link

—

Patchday Android: Angreifer können sich höhere Rechte erschleichen

Android-Geräte sind für Attacken anfällig. Google, Samsung & Co. stellen Sicherheitsupdates bereit.

- Link

—

Update für Google Chrome schließt sechs Sicherheitslücken

Google hat aktualisierte Chrome-Versionen herausgegeben. Sie schließen sechs Sicherheitslücken, davon mehrere mit hohem Risiko.

- Link

—

Lücke in Barracuda E-Mail Security Gateway ermöglichte Code-Einschleusung

Einfallstor für die Sicherheitslücke ist ein Excel-Parser. Barracuda hat bereits Patches auf allen

betroffenen Geräten ausgerollt.
- Link
—
Sicherheitsupdate: Schadcode-Attacken auf Juniper Secure Analytics möglich
Angreifer können Junipers SIEM-System Secure Analytics ins Visier nehmen. Sicherheitspatches sind verfügbar.
- Link
—
Kritische Sicherheitslücke in Perl-Bibliothek: Schwachstelle bereits ausgenutzt
In einer Perl-Bibliothek zum Parsen von Excel-Dateien haben Sicherheitsforscher eine kritische Schwachstelle entdeckt, die Angreifer bereits ausgenutzt haben.
- 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-2023-5360	0.967230000	0.995790000	Link
CVE-2023-4966	0.917920000	0.987020000	Link
CVE-2023-46747	0.965530000	0.995200000	Link
CVE-2023-46604	0.968050000	0.996100000	Link
CVE-2023-42793	0.972830000	0.998350000	Link
CVE-2023-38035	0.971630000	0.997650000	Link
CVE-2023-35078	0.948640000	0.991090000	Link
CVE-2023-34634	0.906880000	0.985840000	Link
CVE-2023-34039	0.921440000	0.987370000	Link
CVE-2023-33246	0.971220000	0.997480000	Link
CVE-2023-32315	0.964530000	0.994780000	Link
CVE-2023-30625	0.939660000	0.989630000	Link
CVE-2023-30013	0.944370000	0.990360000	Link
CVE-2023-28771	0.923800000	0.987740000	Link
CVE-2023-27524	0.906500000	0.985810000	Link
CVE-2023-27372	0.970430000	0.997000000	Link
CVE-2023-27350	0.972290000	0.998030000	Link
CVE-2023-26469	0.938510000	0.989490000	Link
CVE-2023-26360	0.942270000	0.989970000	Link
CVE-2023-26035	0.968020000	0.996080000	Link
CVE-2023-25717	0.954350000	0.992240000	Link
CVE-2023-25194	0.910840000	0.986230000	Link
CVE-2023-2479	0.958820000	0.993240000	Link
CVE-2023-24489	0.968700000	0.996360000	Link
CVE-2023-22518	0.965250000	0.995040000	Link
CVE-2023-22515	0.955290000	0.992450000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21839	0.962040000	0.994030000	Link
CVE-2023-21823	0.940060000	0.989690000	Link
CVE-2023-21554	0.961220000	0.993780000	Link
CVE-2023-20887	0.961530000	0.993850000	Link
CVE-2023-1671	0.953130000	0.991950000	Link
CVE-2023-0669	0.968210000	0.996140000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 08 Jan 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

—

Mon, 08 Jan 2024

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Mon, 08 Jan 2024

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

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

- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] Squid: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] IBM Operational Decision Manager: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in IBM Operational Decision Manager ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Mon, 08 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und Informationen falsch darzustellen.

- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] CUPS: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in CUPS um beliebigen Programmcode auszuführen.

- Link

—

Mon, 08 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 08 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 08 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 08 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

- Link

—

Mon, 08 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung

Ein Angreifer in Funk-Reichweite kann eine Schwachstelle in bluez ausnutzen, um beliebigen Pro-

grammcode auszuführen.
- Link

—

Mon, 08 Jan 2024

[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

—

Mon, 08 Jan 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 08 Jan 2024

[NEU] [hoch] IBM DB2: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in IBM DB2 ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Mon, 08 Jan 2024

[NEU] [hoch] QNAP NAS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in QNAP NAS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.
- Link

—

Fri, 05 Jan 2024

[NEU] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/8/2024	[QNAP QTS / QuTS hero Vulnerability in Netatalk (QSA-23-22)]	critical
1/8/2024	[Siemens SCALANCE Improper Neutralization of Special Elements in Output Used by a Downstream Component (‘Injection’) (CVE-2023-44373)]	critical
1/7/2024	[Adobe Experience Manager 6.0.0.0 < 6.5.19.1 Arbitrary code execution (APSB23-77)]	critical
1/7/2024	[Fedora 38 : perl-Spreadsheet-ParseExcel (2023-84d3cc47b1)]	critical
1/7/2024	[Fedora 39 : perl-Spreadsheet-ParseExcel (2023-921f6975c2)]	critical
1/6/2024	[GLSA-202401-07 : R: Directory Traversal]	critical
1/6/2024	[Fedora 38 : chromium (2024-a6c2300bca)]	critical
1/8/2024	[RHEL 9 : squid (RHSA-2024:0071)]	high
1/8/2024	[RHEL 9 : squid (RHSA-2024:0072)]	high
1/8/2024	[QNAP QTS / QuTS hero Vulnerability in QTS and QuTS hero (QSA-23-64)]	high
1/8/2024	[AlmaLinux 9 : squid (ALSA-2024:0071)]	high
1/8/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : QEMU vulnerabilities (USN-6567-1)]	high
1/8/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libclamunrar vulnerabilities (USN-6569-1)]	high
1/8/2024	[Amazon Linux 2023 : ansible-core, ansible-test (ALAS2023-2024-465)]	high
1/8/2024	[Amazon Linux 2023 : golang, golang-bin, golang-misc (ALAS2023-2024-477)]	high
1/8/2024	[Amazon Linux 2023 : postgresql15, postgresql15-contrib, postgresql15-llvmjit (ALAS2023-2024-464)]	high
1/8/2024	[Amazon Linux 2023 : ghostscript, ghostscript-gtk, ghostscript-tools-dvipdf (ALAS2023-2024-470)]	high

Datum	Schwachstelle	Bewertung
1/8/2024	[Amazon Linux 2023 : squid (ALAS2023-2024-467)]	high
1/8/2024	[Amazon Linux 2023 : jtidy, jtidy-javadoc (ALAS2023-2024-478)]	high
1/8/2024	[Amazon Linux 2023 : p7zip, p7zip-plugins (ALAS2023-2024-481)]	high
1/8/2024	[Amazon Linux 2023 : grpc, grpc-cpp, grpc-data (ALAS2023-2024-474)]	high
1/8/2024	[Amazon Linux 2023 : tar (ALAS2023-2024-475)]	high
1/8/2024	[Amazon Linux 2023 : tomcat9, tomcat9-admin-webapps, tomcat9-el-3.0-api (ALAS2023-2024-471)]	high
1/8/2024	[Phoenix Contact PLCnext Control Insufficient Read and Write Protection to Logic and Runtime Data (CVE-2023-46142)]	high
1/7/2024	[Fedora 39 : tinyxml (2024-80e6578a01)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 08 Jan 2024

iGalerie 3.0.22 Cross Site Scripting

iGalerie version 3.0.22 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Femitter FTP Server 1.03 Denial Of Service

Femitter FTP Server version 1.03 remote denial of service exploit.

- Link

—

” “Mon, 08 Jan 2024

PluXml Blog 5.8.9 Remote Code Execution

PluXml Blog version 5.8.9 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Linux 6.4 io_uring Use-After-Free

Linux versions 6.4 and above suffer from an io_uring page use-after-free vulnerability via buffer ring mmap.

- Link

—

” “Mon, 08 Jan 2024

io_uring __io_uaddr_map() Dangerous Multi-Page Handling

__io_uaddr_map() in io_uring suffers from dangerous handling of the multi-page region.

- Link

—

” “Mon, 08 Jan 2024

Form Tools 3.1.1 Cross Site Scripting

Form Tools version 3.1.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Gom Player 2.3.92.5362 Buffer Overflow

Gom Player version 2.3.92.5362 suffers from a buffer overflow vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Gom Player 2.3.92.5362 DLL Hijacking

Gom Player version 2.3.92.5362 suffers from a dll hijacking vulnerability.

- Link

—

” “Mon, 08 Jan 2024

FreeSWITCH Denial Of Service

FreeSWITCH versions prior to 1.10.11 remote denial of service exploit that leverages a race condition in the hello handshake phase of the DTLS protocol.

- Link

—

” “Sun, 07 Jan 2024

File Sharing Wizard 1.5.0 Denial Of Service

File Sharing Wizard version 1.5.0 remote denial of service exploit.

- Link

—

” “Sat, 06 Jan 2024

httpdx 1.5.4 Denial Of Service

httpdx version 1.5.4 remote denial of service exploit.

- Link

—

” “Fri, 05 Jan 2024

Themebleed Windows 11 Themes Arbitrary Code Execution

When an unpatched Windows 11 host loads a theme file referencing an msstyles file, Windows loads the msstyles file, and if that file’s PACKME_VERSION is 999, it then attempts to load an accompanying dll file ending in _vrf.dll. Before loading that file, it verifies that the file is signed. It does this by opening the file for reading and verifying the signature before opening the file for execution. Because this action is performed in two discrete operations, it opens the procedure for a time of check to time of use vulnerability. By embedding a UNC file path to an SMB server we control, the SMB server can serve a legitimate, signed dll when queried for the read, but then serve a different file of the same name when the host intends to load/execute the dll.

- Link

—

” “Fri, 05 Jan 2024

Easy Chat Server 3.1 Denial Of Service

Easy Chat Server version 3.1 suffers from a denial of service vulnerability.

- Link

—

” “Thu, 04 Jan 2024

Easy File Sharing FTP Server 2.0 Denial Of Service

Easy File Sharing FTP Server version 2.0 suffers from a denial of service vulnerability.

- Link

—

” “Wed, 03 Jan 2024

minaliC 2.0.0 Denial Of Service

minaliC version 2.0.0 suffers from a denial of service vulnerability.

- Link

—

” “Wed, 03 Jan 2024

Microsoft Windows Kernel Information Disclosure

Any unprivileged, local user in Microsoft Windows can disclose whether a specific file, directory or registry key exists in the system or not, even if they do not have the open right to it or enumerate right to its parent.

- Link

—

” “Wed, 03 Jan 2024

Chrome BindTextSuggestionHostForFrame Type Confusion

Chrome suffers from a type confusion vulnerability in BindTextSuggestionHostForFrame.

- Link

—

” “Wed, 03 Jan 2024

WebCalendar 1.3.0 Cross Site Scripting

WebCalendar version 1.3.0 suffers from reflective and persistent cross site scripting vulnerabilities.

- Link

—

” “Wed, 03 Jan 2024

CMSMS 2.2.19 Arbitrary File Upload

CMSMS version 2.2.19 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Tue, 02 Jan 2024

Packet Storm New Exploits For 2023

Complete comprehensive archive of all 1,863 exploits added to Packet Storm in 2023.

- Link

—

” “Tue, 02 Jan 2024

Packet Storm New Exploits For December, 2023

This archive contains all of the 74 exploits added to Packet Storm in December, 2023.

- Link

—

” “Tue, 02 Jan 2024

Apache 2.4.55 mod_proxy HTTP Request Smuggling

Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow for an HTTP request smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

- Link

—

” “Tue, 02 Jan 2024

FTPDMIN 0.96 Denial Of Service

FTPDMIN version 0.96 suffers from a denial of service vulnerability.
- Link
—
” “Tue, 02 Jan 2024
Ultra Mini HTTPd 1.21 Denial Of Service
Ultra Mini HTTPd version 1.21 suffers from a denial of service vulnerability.
- Link
—
” “Fri, 29 Dec 2023
Apache OFBiz 18.12.09 Remote Code Execution
Apache OFBiz version 18.12.09 suffers from a pre-authentication remote code execution vulnerability.
- Link
—
”

4.2 0-Days der letzten 5 Tage

“Fri, 05 Jan 2024
ZDI-24-018: Inductive Automation Ignition ExtendedDocumentCodec Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Fri, 05 Jan 2024
ZDI-24-017: Inductive Automation Ignition ResponseParser Notification Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Fri, 05 Jan 2024
ZDI-24-016: Inductive Automation Ignition ResponseParser SerializedResponse Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Fri, 05 Jan 2024
ZDI-24-015: Inductive Automation Ignition Base64Element Deserialization of Untrusted Data Remote Code Execution Vulnerability
- Link
—
” “Fri, 05 Jan 2024

ZDI-24-014: Inductive Automation Ignition RunQuery Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

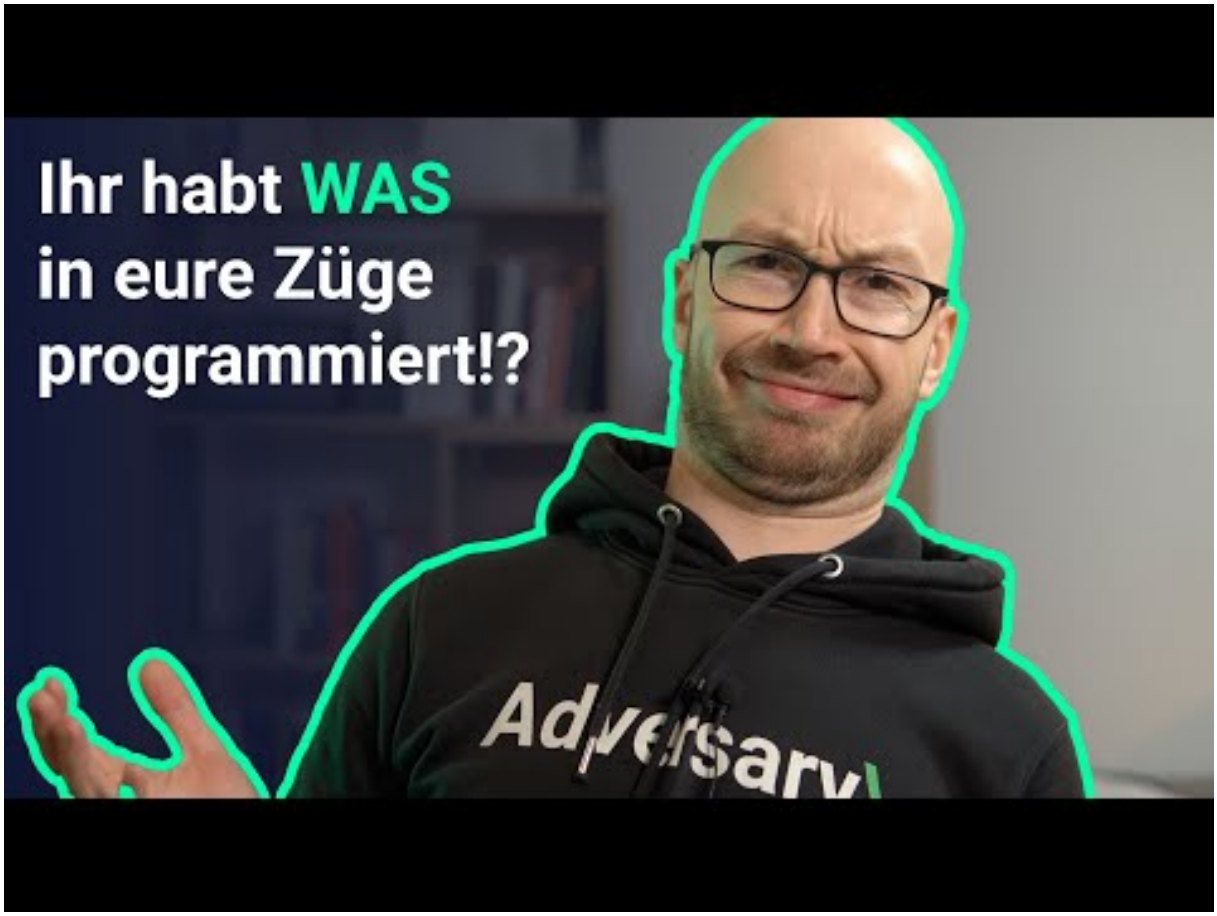
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Ihr habt WAS in eure Züge programmiert!?



Zum Youtube Video

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-06	loanDepot	[USA]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-16	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	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.