Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240102

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 . . . 16

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 **17**
8.1 Quellenverzeichnis . . . 17

9 Impressum **18**

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 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

—

Kritische Lücken in Mobile-Device-Management-Lösung Ivanti Avalanche geschlossen

Angreifer können Ivanti Avalanche mit Schadcode attackieren. Eine reparierte Version steht zum Download bereit.

- Link

—

Google Chrome: Zero-Day-Lücke wird angegriffen, Update verfügbar

Googles Entwickler haben ein Update für Chrome veröffentlicht, das eine bereits angegriffene Sicherheitslücke abdichtet.

- Link

—

Firefox und Thunderbird: Sicherheitslücken geschlossen und Funktionen ergänzt

Die neuen Versionen von Firefox und Thunderbird dichten Sicherheitslecks ab. Zudem bringen sie neue Funktionen mit.

- Link

—

Jetzt patchen! Botnetz InfectedSlurs hat es auf Qnap NAS abgesehen

Eine Sicherheitslücke in der IP-Kamera-Software VioStor NVR auf Netzwerkspeichern von Qnap dient als Schlupfloch für Malware.

- Link

—

Sicherheitsupdates: Fortinet schützt Firewalls & Co. vor möglichen Attacken

Der Netzwerkausrüster Fortinet hat in mehreren Produkten gefährliche Lücken geschlossen.

- Link

—

Squid-Proxy: Denial of Service durch Endlosschleife

Schickt ein Angreifer einen präparierten HTTP-Header an den Proxy-Server, kann er ihn durch eine unkontrollierte Rekursion zum Stillstand bringen.

- Link

—

Zoom behebt Sicherheitslücken unter Windows, Android und iOS

Durch ungenügende Zugriffskontrolle, Verschlüsselungsprobleme und Pfadmanipulation konnten Angreifer sich zusätzliche Rechte verschaffen.

- Link

—

Patchday: Adobe schließt 185 Sicherheitslücken in Experience Manager

Angreifer können Systeme mit Anwendungen von Adobe ins Visier nehmen. Nun hat der Softwarehersteller Schwachstellen geschlossen.

- Link

—

Patchday Microsoft: Outlook kann sich an Schadcode-E-Mail verschlucken

Microsoft hat wichtige Sicherheitsupdates für Azure, Defender & Co. veröffentlicht. Bislang soll es keine Attacken geben.

- 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	0.968720000	0.996320000	Link
CVE-2023-4966	0.917920000	0.986830000	Link
CVE-2023-46747	0.965530000	0.995100000	Link
CVE-2023-46604	0.968050000	0.996050000	Link
CVE-2023-42793	0.972640000	0.998190000	Link
CVE-2023-38035	0.970940000	0.997240000	Link
CVE-2023-35078	0.953010000	0.991780000	Link
CVE-2023-34634	0.900470000	0.985230000	Link
CVE-2023-34039	0.928890000	0.988160000	Link
CVE-2023-33246	0.971220000	0.997420000	Link
CVE-2023-32315	0.961510000	0.993720000	Link
CVE-2023-30625	0.941420000	0.989750000	Link
CVE-2023-30013	0.925700000	0.987810000	Link
CVE-2023-28771	0.923800000	0.987590000	Link
CVE-2023-27524	0.906990000	0.985610000	Link
CVE-2023-27372	0.971560000	0.997580000	Link
CVE-2023-27350	0.972290000	0.997990000	Link
CVE-2023-26469	0.933320000	0.988700000	Link
CVE-2023-26360	0.934340000	0.988830000	Link
CVE-2023-25717	0.962820000	0.994090000	Link
CVE-2023-25194	0.908370000	0.985750000	Link
CVE-2023-2479	0.958820000	0.993110000	Link
CVE-2023-24489	0.967670000	0.995930000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22518	0.967630000	0.995920000	Link
CVE-2023-22515	0.955290000	0.992300000	Link
CVE-2023-21839	0.960570000	0.993480000	Link
CVE-2023-21823	0.955130000	0.992240000	Link
CVE-2023-21554	0.961220000	0.993620000	Link
CVE-2023-20887	0.957180000	0.992700000	Link
CVE-2023-1671	0.952600000	0.991690000	Link
CVE-2023-0669	0.966690000	0.995500000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 29 Dec 2023

[UPDATE] [hoch] GStreamer: Mehrere Schwachstellen

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

- Link

—

Fri, 29 Dec 2023

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 28 Dec 2023

[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

—

Thu, 28 Dec 2023

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- Link

—

Thu, 28 Dec 2023

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- Link

—

Thu, 28 Dec 2023

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Daten zu manipulieren und seine Privilegien zu erweitern.

- Link

—

Thu, 28 Dec 2023

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 28 Dec 2023

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

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 27 Dec 2023

[NEU] [kritisch] Barracuda Networks Email Security Gateway: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Barracuda Networks Email Security Gateway ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 27 Dec 2023

[NEU] [hoch] Cacti: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentifizierter Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um vertrauliche Informationen offenzulegen, Dateien zu manipulieren und beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder XSS-Angriffe durchzuführen.

- Link

—

Wed, 27 Dec 2023

[NEU] [hoch] ILIAS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in ILIAS ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] ffmpeg: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] PostgreSQL JDBC Treiber: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle im PostgreSQL JDBC Treiber ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 27 Dec 2023

[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

—

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat Enterprise Linux (flatpak): Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in flatpak ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode auszuführen, ein Cross-Site-Scritping-Angriff durchzuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat Enterprise Linux Ceph Storage: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux Ceph Storage ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] Oracle Fusion Middleware: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Fusion Middleware ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Wed, 27 Dec 2023

[UPDATE] [hoch] Red Hat Integration Camel for Spring Boot: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Integration Camel for Spring Boot ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
12/30/2023	[openSUSE 15 Security Update : deepin-compressor (openSUSE-SU-2023:0424-1)]	critical
12/30/2023	[openSUSE 15 Security Update : deepin-compressor (openSUSE-SU-2023:0423-1)]	critical
12/28/2023	[Microsoft Windows 10 1507 SEoL]	critical
12/27/2023	[NewStart CGSL MAIN 6.06 : gnutls Multiple Vulnerabilities (NS-SA-2023-0100)]	critical
12/27/2023	[GLSA-202312-17 : OpenSSH: Multiple Vulnerabilities]	critical
12/30/2023	[Fedora 38 : xerces-c (2023-52ba628e03)]	high
12/30/2023	[Fedora 39 : xerces-c (2023-817ecc703f)]	high
12/29/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postfix (SUSE-SU-2023:4981-1)]	high
12/29/2023	[openSUSE 15 Security Update : zabbix (openSUSE-SU-2023:0418-1)]	high
12/29/2023	[openSUSE 15 Security Update : zabbix (openSUSE-SU-2023:0419-1)]	high
12/29/2023	[SUSE SLED12 / SLES12 Security Update : libreoffice (SUSE-SU-2023:4984-1)]	high
12/29/2023	[SUSE SLES12 Security Update : gstreamer (SUSE-SU-2023:4982-1)]	high
12/28/2023	[SUSE SLED12 / SLES12 Security Update : webkit2gtk3 (SUSE-SU-2023:4978-1)]	high
12/28/2023	[SUSE SLES15 Security Update : gstreamer (SUSE-SU-2023:4980-1)]	high
12/28/2023	[Plantronics Hub < 3.25.1 Privilege Escalation]	high
12/28/2023	[Fedora 39 : squid (2023-ab77331a34)]	high
12/28/2023	[Fedora 38 : squid (2023-6317eaa767)]	high
12/28/2023	[Moxa (CVE-2023-5961)]	high

Datum	Schwachstelle	Bewertung
12/27/2023	[NewStart CGSL MAIN 6.06 : dhcp Vulnerability (NS-SA-2023-0091)]	high
12/27/2023	[NewStart CGSL MAIN 6.06 : cpio Vulnerability (NS-SA-2023-0088)]	high
12/27/2023	[NewStart CGSL MAIN 6.02 : kernel Multiple Vulnerabilities (NS-SA-2023-0107)]	high
12/27/2023	[NewStart CGSL MAIN 6.02 : kernel Multiple Vulnerabilities (NS-SA-2023-0105)]	high
12/27/2023	[NewStart CGSL MAIN 5.04 : gzip Vulnerability (NS-SA-2023-0103)]	high
1/1/2024	[openSUSE 15 Security Update : opera (openSUSE-SU-2024:0001-1)]	high
1/1/2024	[openSUSE 15 Security Update : opera (openSUSE-SU-2024:0002-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Thu, 28 Dec 2023

Microsoft Windows PowerShell Code Execution / Event Log Bypass

Prior work from this researcher disclosed how PowerShell executes unintended files or BASE64 code when processing specially crafted filenames. This research builds on their PSTrojanFile work, adding a PS command line single quote bypass and PS event logging failure. On Windows CL tab, completing a filename uses double quotes that can be leveraged to trigger arbitrary code execution. However, if the filename got wrapped in single quotes it failed, that is until now.

- Link

—

” “Thu, 28 Dec 2023

Lot Reservation Management System 1.0 Shell Upload

Lot Reservation Management System version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Thu, 28 Dec 2023

Lot Reservation Management System 1.0 File Disclosure

Lot Reservation Management System version 1.0 suffers from a file disclosure vulnerability.

- Link

—

” “Wed, 27 Dec 2023

WhatACart 2.0.7 Cross Site Scripting

WhatACart version 2.0.7 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 26 Dec 2023

ShopSite 14.0 Cross Site Scripting

ShopSite version 14.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 26 Dec 2023

FreeSWITCH 1.10.10 Denial Of Service

When handling DTLS-SRTP for media setup, FreeSWITCH version 1.10.10 is susceptible to denial of service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack.

- Link

—

” “Fri, 22 Dec 2023

Craft CMS 4.4.14 Remote Code Execution

This Metasploit module exploits an unauthenticated remote code execution vulnerability in Craft CMS versions 4.0.0-RC1 through 4.4.14.

- Link

—

” “Fri, 22 Dec 2023

Hospital Management System 4.0 XSS / Shell Upload / SQL Injection

Hospital Management System versions 4.0 and below suffer from cross site scripting, remote shell upload, and remote SQL injection vulnerabilities.

- Link

—

” “Fri, 22 Dec 2023

GilaCMS 1.15.4 SQL Injection

GilaCMS versions 1.15.4 and below suffer from multiple remote SQL injection vulnerabilities.

- Link

—

” “Thu, 21 Dec 2023

Vinchin Backup And Recovery Command Injection

This Metasploit module exploits a command injection vulnerability in Vinchin Backup & Recovery v5.0*., v6.0.*, v6.7*., and v7.0.*. Due to insufficient input validation in the checkIpExists API endpoint, an attacker can execute arbitrary commands as the web server user.

- Link

—

” “Thu, 21 Dec 2023

Glibc Tunables Privilege Escalation

A buffer overflow exists in the GNU C Library’s dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. It has been dubbed Looney Tunables. This issue allows an local attacker to use maliciously crafted GLIBC_TUNABLES when launching binaries with SUID permission to execute code in the context of the root user. This Metasploit module targets glibc packaged on Ubuntu and Debian. Fedora 37 and 38 and other distributions of linux also come packaged with versions of glibc vulnerable to CVE-2023-4911 however this module does not target them.

- Link

—

” “Wed, 20 Dec 2023

MOKOSmart MKGW1 Gateway Improper Session Management

MOKOSmart MKGW1 Gateway devices with firmware version 1.1.1 or below do not provide an adequate session management for the administrative web interface. This allows adjacent attackers with access to the management network to read and modify the configuration of the device.

- Link

—

” “Wed, 20 Dec 2023

TYPO3 11.5.24 Path Traversal

TYPO3 version 11.5.24 suffers from a path traversal vulnerability.

- Link

—

” “Wed, 20 Dec 2023

MajorDoMo Remote Code Execution

MajorDoMo versions prior to 0662e5e suffer from an unauthenticated remote code execution vulnerability.

- Link

—

” “Wed, 20 Dec 2023

Terrapin SSH Connection Weakening

In this paper, the authors show that as new encryption algorithms and mitigations were added to SSH, the SSH Binary Packet Protocol is no longer a secure channel: SSH channel integrity (INT-PST) is broken for three widely used encryption modes. This allows prefix truncation attacks where some encrypted packets at the beginning of the SSH channel can be deleted without the client or server noticing it. They demonstrate several real-world applications of this attack. They show that they can fully break SSH extension negotiation (RFC 8308), such that an attacker can downgrade the public key algorithms for user authentication or turn off a new countermeasure against keystroke timing attacks introduced in OpenSSH 9.5. They also identified an implementation flaw in AsyncSSH that, together with prefix truncation, allows an attacker to redirect the victim’s login into a shell controlled by the attacker. Related proof of concept code from their github has been added to this archive.

- Link

—

” “Tue, 19 Dec 2023

Atlassian Confluence Improper Authorization / Code Execution

This improper authorization vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to the Confluence instance administrator. This Metasploit module uses the administrator account to install a malicious .jsp servlet plugin which the user can trigger to gain code execution on the target in the context of the of the user running the confluence server.

- Link

—

” “Fri, 15 Dec 2023

RTPEngine mr11.5.1.6 Denial Of Service

RTPEngine version mr11.5.1.6 suffers from a denial of service vulnerability via DTLS Hello packets during call initiation.

- Link

—

” “Fri, 15 Dec 2023

PKP-WAL 3.4.0-3 Remote Code Execution

PKP Web Application Library (PKP-WAL) versions 3.4.0-3 and below, as used in Open Journal Systems (OJS), Open Monograph Press (OMP), and Open Preprint Systems (OPS) before versions 3.4.0-4 or

3.3.0-16, suffer from a NativeImportExportPlugin related remote code execution vulnerability.
- Link

—

” “Fri, 15 Dec 2023

Asterisk 20.1.0 Denial Of Service

When handling DTLS-SRTP for media setup, Asterisk version 20.1.0 is susceptible to denial of service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack.
- Link

—

” “Fri, 15 Dec 2023

osCommerce 4.13-60075 Shell Upload

osCommerce version 4.13-60075 suffers from a remote shell upload vulnerability.
- Link

—

” “Thu, 14 Dec 2023

Chrome V8 Sandbox Escape

Proof of concept exploit for a new technique to escape from the Chrome V8 sandbox.
- Link

—

” “Thu, 14 Dec 2023

Chrome V8 Type Confusion / New Sandbox Escape

Proof of concept exploit for CVE-2023-3079 that leverages a type confusion in V8 in Google Chrome versions prior to 114.0.5735.110. This issue allows a remote attacker to potentially exploit heap corruption via a crafted HTML page. This variant of the exploit applies a new technique to escape the sandbox.
- Link

—

” “Thu, 14 Dec 2023

Chrome V8 JIT XOR Arbitrary Code Execution

Chrome V8 proof of concept exploit for CVE-2021-21220. The specific flaw exists within the implementation of XOR operation when executed within JIT compiled code.
- Link

—

” “Thu, 14 Dec 2023

Chrome V8 Type Confusion

Proof of concept exploit for CVE-2023-3079 that leverages a type confusion in V8 in Google Chrome versions prior to 114.0.5735.110. This issue allows a remote attacker to potentially exploit heap

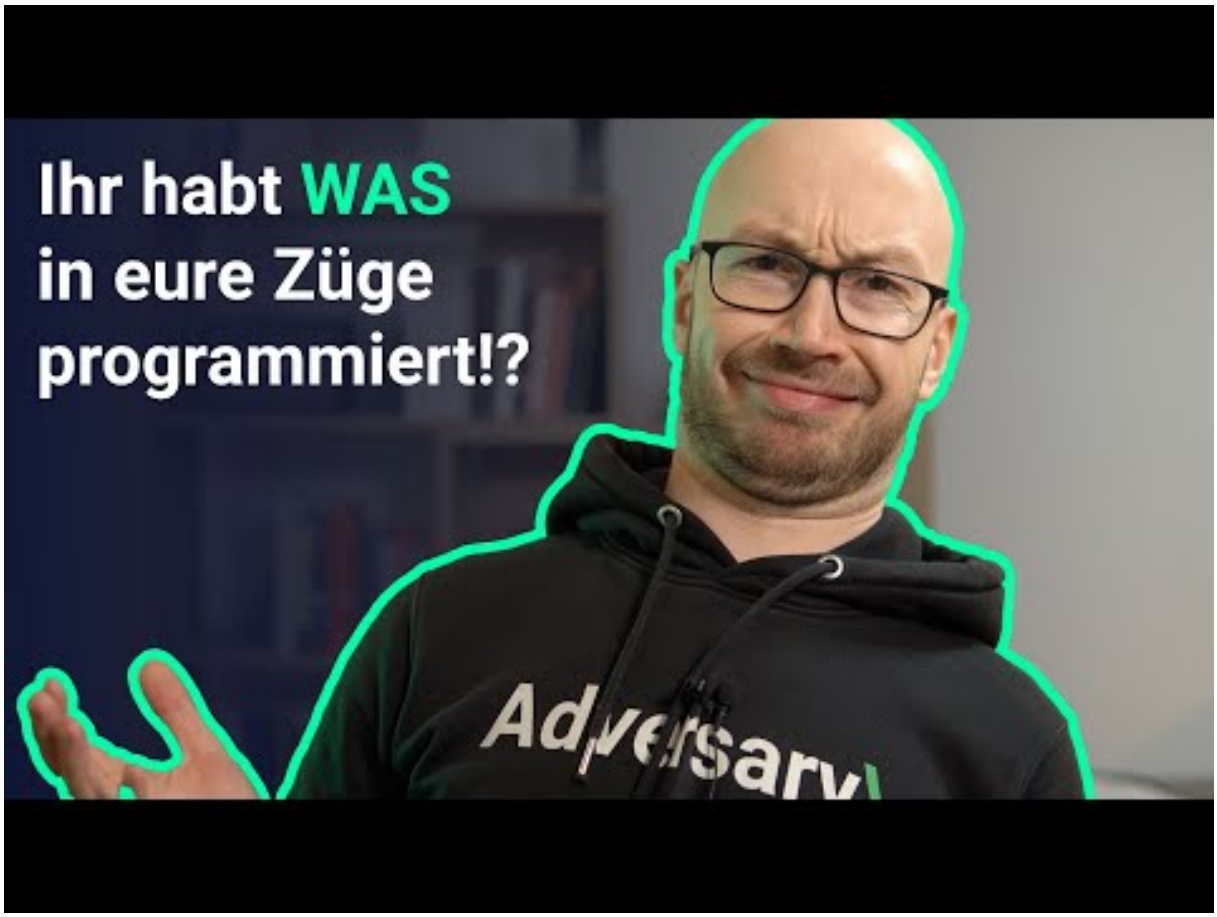
corruption via a crafted HTML page.
- Link
—
”

4.2 0-Days der letzten 5 Tage

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

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Grupppe	Webseite
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

Abbildung 1: Marlon Hübner

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.