Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240202

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

Mastodon: Diebstahl beliebiger Identitäten im föderierten Kurznachrichtendienst
In einem knappen Sicherheitshinweis lassen die Entwickler eine Bombe platzen: Angreifer können jeden beliebigen Account übernehmen und fälschen.
- Link

—

Ivanti: Updates mit Verspätung, dafür neue Sicherheitslücke missbraucht
Ivanti hat Updates zum Schließen von Sicherheitslücken veröffentlicht, die bereits angegriffen werden. Zwei weitere Lecks sind dabei aufgetaucht.
- Link

—

Linux: Sicherheitslücke in glibc bringt Angreifern Root-Privilegien
Fast alle aktuellen Linux-Varianten sind von dem Sicherheitsleck betroffen, das Missetäter jedoch nicht aus der Ferne angreifen können. Updates stehen bereit.
- Link

—

Sicherheitsupdates: DoS- und Schadcode-Attacken auf IBM ODM möglich
Angreifer können Systeme über diverse Schwachstellen in IBM Operational Decision Manager kompromittieren.
- Link

—

Google Chrome: Update schließt vier Sicherheitslücken
Google hat mit dem wöchentlichen Chrome-Update vier Sicherheitslücken geschlossen. Sie könnten das Einschleusen von Schadcode erlauben.
- Link

—

Jetzt updaten! Exploits für kritische Jenkins-Sicherheitslücke im Umlauf
Für die in der vergangenen Woche bekanntgewordene kritische Sicherheitslücke in Jenkins ist Exploit-Code aufgetaucht. Höchste Zeit zum Aktualisieren!
- Link

—

Schadcode-Attacken auf Onlineshops auf Gambio-Basis möglich
Admins von Onlineshops sollten die Gambio-Software aus Sicherheitsgründen auf den aktuellen Stand bringen.
- Link

—

Diesmal bitte patchen: Security-Update behebt kritische Schwachstelle in GitLab

GitLab 16.x enthält fünf Schwachstellen, von denen eine als kritisch eingestuft ist. Patchen ist nicht selbstverständlich, wie jüngst eine Untersuchung zeigte.

- Link

—

Microsoft Edge 121 unterstützt moderne Codecs und stopft Sicherheitslecks

Microsoft hat den Webbrowser Edge in Version 121 herausgegeben. Sie stopft eine kritische Sicherheitslücke und liefert Support für AV1-Videos.

- Link

—

Angreifer können eigene Befehle auf Juniper-Firewalls und Switches ausführen

Entwickler von Juniper haben in Junos OS mehrere Sicherheitslücken geschlossen. Noch sind aber nicht alle Updates 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-2023-6553	0.909010000	0.986360000	Link
CVE-2023-5360	0.967230000	0.995910000	Link
CVE-2023-4966	0.931240000	0.988830000	Link
CVE-2023-46805	0.930450000	0.988740000	Link
CVE-2023-46747	0.970150000	0.996970000	Link
CVE-2023-46604	0.971470000	0.997610000	Link
CVE-2023-42793	0.973260000	0.998690000	Link
CVE-2023-38035	0.971870000	0.997830000	Link
CVE-2023-35082	0.932740000	0.989060000	Link
CVE-2023-35078	0.955550000	0.992660000	Link
CVE-2023-34634	0.906880000	0.986130000	Link
CVE-2023-34362	0.952300000	0.991910000	Link
CVE-2023-33246	0.971270000	0.997530000	Link
CVE-2023-32315	0.963290000	0.994510000	Link
CVE-2023-30625	0.937630000	0.989580000	Link
CVE-2023-30013	0.925700000	0.988220000	Link
CVE-2023-29300	0.939750000	0.989830000	Link
CVE-2023-28771	0.923800000	0.987960000	Link
CVE-2023-27524	0.961820000	0.994070000	Link
CVE-2023-27372	0.970420000	0.997110000	Link
CVE-2023-27350	0.972430000	0.998160000	Link
CVE-2023-26469	0.927230000	0.988400000	Link
CVE-2023-26360	0.943910000	0.990480000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-26035	0.968710000	0.996480000	Link
CVE-2023-25717	0.956130000	0.992770000	Link
CVE-2023-25194	0.916080000	0.987030000	Link
CVE-2023-2479	0.958820000	0.993360000	Link
CVE-2023-24489	0.968380000	0.996330000	Link
CVE-2023-23752	0.963140000	0.994440000	Link
CVE-2023-23397	0.906590000	0.986100000	Link
CVE-2023-22527	0.973010000	0.998510000	Link
CVE-2023-22518	0.965250000	0.995170000	Link
CVE-2023-22515	0.956820000	0.992930000	Link
CVE-2023-21839	0.957980000	0.993160000	Link
CVE-2023-21823	0.940060000	0.989880000	Link
CVE-2023-21554	0.961220000	0.993880000	Link
CVE-2023-20887	0.962660000	0.994260000	Link
CVE-2023-20198	0.924070000	0.988010000	Link
CVE-2023-1671	0.953130000	0.992100000	Link
CVE-2023-0669	0.968210000	0.996270000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 01 Feb 2024

[NEU] [hoch] docker: Mehrere Schwachstellen

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

- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] Rockwell Automation ControlLogix: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] Rockwell Automation FactoryTalk: Schwachstelle ermöglicht Manipulation von Dateien und Offenlegung von Informationen

Ein anonymer Angreifer kann eine Schwachstelle in Rockwell Automation FactoryTalk ausnutzen, um Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] D-LINK COVR-2600R & COVR-3902: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in COVR-2600R & COVR-3902 Routern ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] Sparx Systems Enterprise Architect: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in Sparx Systems Enterprise Architect ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 01 Feb 2024

[NEU] [hoch] D-LINK Router: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [kritisch] Apple macOS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um den Benutzer zu täuschen, Informationen offenzulegen, Sicherheitsmechanismen zu umgehen, Rechte zu erweitern und beliebigen Code mit Kernel-Rechten auszuführen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Apple iOS: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen Informationen offenzulegen oder einen Denial of Service zu verursachen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen und potenziell, um Code auszuführen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 01 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen und potenziell, um Code auszuführen.

- Link

—

Thu, 01 Feb 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 oder um andere, nicht näher spezifizierte Auswirkungen zu erzielen.

- Link

—

Thu, 01 Feb 2024

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

Ein entfernter anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann diese Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen und Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Google Chrome / 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

—

Thu, 01 Feb 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge

ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Thu, 01 Feb 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
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/1/2024	[Fedora 38 : python-templated-dictionary (2024-4bd03c989b)]	critical
2/1/2024	[SUSE SLES15 Security Update : slurm (SUSE-SU-2024:0279-1)]	critical
2/1/2024	[openSUSE 15 Security Update : slurm_20_02 (SUSE-SU-2024:0278-1)]	critical
2/1/2024	[SUSE SLES15 / openSUSE 15 Security Update : slurm_22_05 (SUSE-SU-2024:0283-1)]	critical
2/1/2024	[SUSE SLES15 / openSUSE 15 Security Update : slurm_20_11 (SUSE-SU-2024:0288-1)]	critical
2/1/2024	[SUSE SLES15 Security Update : slurm_23_02 (SUSE-SU-2024:0280-1)]	critical
2/1/2024	[SUSE SLES15 Security Update : slurm (SUSE-SU-2024:0287-1)]	critical
2/1/2024	[SUSE SLES15 / openSUSE 15 Security Update : slurm (SUSE-SU-2024:0284-1)]	critical

Datum	Schwachstelle	Bewertung
2/1/2024	[SUSE SLES15 Security Update : slurm_22_05 (SUSE-SU-2024:0286-1)]	critical
2/1/2024	[SUSE SLES15 Security Update : slurm_23_02 (SUSE-SU-2024:0289-1)]	critical
2/1/2024	[Oracle Linux 8 : tigervnc (ELSA-2024-0607)]	critical
2/1/2024	[FreeBSD : qt6-webengine – Multiple vulnerabilities (bbcb1584-c068-11ee-bdd6-4ccc6adda413)]	critical
2/1/2024	[Oracle Linux 7 : tigervnc (ELSA-2024-0629)]	critical
2/2/2024	[Debian dsa-5613 : openjdk-17-dbg - security update]	high
2/1/2024	[Fedora 39 : thunderbird (2024-c8c2a52fb8)]	high
2/1/2024	[Fedora 38 : glibc (2024-07597a0fb3)]	high
2/1/2024	[Debian dla-3729 : debian-security-support - security update]	high
2/1/2024	[Amazon Linux AMI : runc (ALAS-2024-1911)]	high
2/1/2024	[Amazon Linux 2 : runc (ALASNITRO-ENCLAVES-2024-036)]	high
2/1/2024	[Amazon Linux 2 : runc (ALASECS-2024-033)]	high
2/1/2024	[Amazon Linux 2023 : runc (ALAS2023-2024-501)]	high
2/1/2024	[Amazon Linux 2 : runc (ALASDOCKER-2024-036)]	high
2/1/2024	[Arista Networks EOS DoS (SA0087)]	high
2/1/2024	[Dell iDRAC Service Module < 5.3.0.0 Privilege Escalation]	high
2/1/2024	[FreeBSD : lizard – Negative size passed to memcpy resulting in memory corruption (67c2eb06-5579-4595-801b-30355be24654)]	high
2/1/2024	[Ubuntu 23.10 : GNU C Library vulnerabilities (USN-6620-1)]	high
2/1/2024	[AlmaLinux 9 : thunderbird (ALSA-2024:0602)]	high
2/1/2024	[AlmaLinux 9 : firefox (ALSA-2024:0603)]	high
2/1/2024	[AlmaLinux 8 : gnutls (ALSA-2024:0627)]	high
2/1/2024	[AlmaLinux 8 : thunderbird (ALSA-2024:0609)]	high
2/1/2024	[AlmaLinux 8 : firefox (ALSA-2024:0608)]	high

Datum	Schwachstelle	Bewertung
2/1/2024	[Debian dla-3731 : man-db - security update]	high
2/1/2024	[Debian dsa-5612 : chromium - security update]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 01 Feb 2024

Packet Storm New Exploits For January, 2024

This archive contains all of the 140 exploits added to Packet Storm in January, 2024.

- Link

—

” “Thu, 01 Feb 2024

Apache Tomcat 8.5.63 / 9.0.43 HTTP Response Smuggling

Apache Tomcat suffers from a client-side de-sync vulnerability via HTTP request smuggling. Apache Tomcat versions 8.5.7 through 8.5.63 and 9.0.0-M11 through 9.0.43 are vulnerable.

- Link

—

” “Thu, 01 Feb 2024

GlobalScape Secure FTP Server 3.0 Denial Of Service

GlobalScape Secure FTP Server version 3.0 remote denial of service exploit.

- Link

—

” “Wed, 31 Jan 2024

XenForo 2.2.13 ArchiveImport.php Zip Slip

XenForo versions 2.2.13 and below suffer from a zip slip filename traversal vulnerability in ArchiveImport.php.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Insecure Access Control

TELSAT marKoni FM Transmitter version 1.9.5 allows an unauthorized user to change passwords.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Client-Side Access Control Bypass

TELSAT marKoni FM Transmitter version 1.9.5 implements client-side restrictions that can be bypassed by editing the HTML source page that enable administrative operations.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Backdoor Account

TELSAT marKoni FM Transmitter version 1.9.5 has a hidden super administrative account factory that has the hardcoded password inokram25 that allows full access to the web management interface configuration.

- Link

—

” “Wed, 31 Jan 2024

TELSAT marKoni FM Transmitter 1.9.5 Root Command Injection

TELSAT marKoni FM Transmitter version 1.9.5 is susceptible to unauthenticated remote code execution with root privileges. An attacker can exploit a command injection vulnerability by manipulating the Email settings’ WAN IP info service, which utilizes the wget module. This allows the attacker to gain unauthorized access to the system with administrative privileges by exploiting the url parameter in the HTTP GET request to ekafcgi.fcgi.

- Link

—

” “Wed, 31 Jan 2024

glibc syslog() Heap-Based Buffer Overflow

Qualys discovered a heap-based buffer overflow in the GNU C Library’s __vsyslog_internal() function, which is called by both syslog() and vsyslog(). This vulnerability was introduced in glibc 2.37 (in August 2022).

- Link

—

” “Wed, 31 Jan 2024

glibc qsort() Out-Of-Bounds Read / Write

Qualys discovered a memory corruption in the glibc’s qsort() function, due to a missing bounds check. To be vulnerable, a program must call qsort() with a nontransitive comparison function (a function cmp(int a, int b) that returns (a - b), for example) and with a large number of attacker-controlled elements (to cause a malloc() failure inside qsort()). They have not tried to find such a vulnerable program in the real world. All glibc versions from at least September 1992 (glibc 1.04) to the current release (glibc 2.38) are affected, but the glibc’s developers have independently discovered and patched this memory corruption in the master branch (commit b9390ba, ”stdlib: Fix array bounds protection in

insertion sort phase of qsort”) during a recent refactoring of qsort().

- Link

—

” “Wed, 31 Jan 2024

Trojan.Win32 BankShot MVID-2024-0669 Buffer Overflow

Trojan.Win32 BankShot malware suffers from a buffer overflow vulnerability.

- Link

—

” “Wed, 31 Jan 2024

War-FTPD 1.65 Denial Of Service

War-FTPD version 1.65 remote denial of service exploit.

- Link

—

” “Wed, 31 Jan 2024

Solar FTP Server 2.1.1 Denial Of Service

Solar FTP Server version 2.1.1 remote denial of service exploit.

- Link

—

” “Wed, 31 Jan 2024

Mirth Connect 4.4.0 Remote Command Execution

A vulnerability exists within Mirth Connect due to its mishandling of deserialized data. This vulnerability can be leveraged by an attacker using a crafted HTTP request to execute OS commands within the context of the target application. The original vulnerability was identified by IHTeam and assigned CVE-2023-37679. Later, researchers from Horizon3.ai determined the patch to be incomplete and published a gadget chain which bypassed the deny list that the original had implemented. This second vulnerability was assigned CVE-2023-43208 and was patched in Mirth Connect version 4.4.1. This Metasploit module has been tested on versions 4.1.1, 4.3.0 and 4.4.0.

- Link

—

” “Tue, 30 Jan 2024

WS_FTP Server 5.0.5 Denial Of Service

WS_FTP Server version 5.0.5 remote denial of service exploit.

- Link

—

” “Tue, 30 Jan 2024

httpdx 1.5.1 Denial Of Service

httpdx version 1.5.1 remote denial of service exploit.

- Link

—

” “Mon, 29 Jan 2024

Reprise License Manager 15.1 Privilege Escalation / File Write

Reprise License Manager version 15.1 suffers from privilege escalation and arbitrary file write vulnerabilities.

- Link

—

” “Mon, 29 Jan 2024

Jenkins 2.441 / LTS 2.426.3 Arbitrary File Read

Jenkins versions 2.441 and below and LTS 2.426.3 and below remote arbitrary file read proof of concept exploit written in Python.

- Link

—

” “Mon, 29 Jan 2024

Jenkins 2.441 / LTS 2.426.3 CVE-2024-23897 Scanner

Jenkins versions 2.441 and LTS 2.426.3 arbitrary file read scanner.

- Link

—

” “Mon, 29 Jan 2024

CSZCMS 1.3.0 SQL Injection

CSZCMS version 1.3.0 suffers from a remote SQL injection vulnerability in the admin flows.

- Link

—

” “Mon, 29 Jan 2024

PrommetriX Prometheus Metrics Leaker

PrommetriX is a tool that demonstrates a data leakage vulnerability in the Prometheus metrics-based event monitoring software.

- Link

—

” “Mon, 29 Jan 2024

Interactive Floor Plan 1.0 Cross Site Scripting

Interactive Floor Plan version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 29 Jan 2024

Chrome 121 Javascript Fork Malloc Bomb

Chrome version 121 suffers from a javascript fork malloc vulnerability that indicates memory corruption upon crash.

- Link

—

” “Mon, 29 Jan 2024

PHPJ Callback Widget 1.0 Cross Site Scripting

PHPJ Callback Widget version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 29 Jan 2024

Xitami 2.5b4 Denial Of Service

Xitami version 2.5b4 remote denial of service exploit.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 31 Jan 2024

ZDI-24-084: (Pwn2Own) Lexmark CX331adwe Missing Authentication Remote Code Execution Vulnerability

- Link

—

” “Wed, 31 Jan 2024

ZDI-24-083: (Pwn2Own) Lexmark CX331adwe PostScript File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Wed, 31 Jan 2024

ZDI-24-082: (Pwn2Own) Lexmark CX331adwe PDF File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Wed, 31 Jan 2024

ZDI-24-081: (Pwn2Own) Lexmark CX331adwe make42charstring Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Microsoft kriegt IHRE EIGENE Cloud nicht sicher konfiguriert

Zum Youtube Video

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Institut des Statistiques d'Albanie (INSTAT)	[ALB]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-02	[Innovex Downhole Solutions]	play	Link
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	Link
2024-02-01	[DIROX LTDA (Vietnã)]	knight	Link
2024-02-01	[etsolutions.com.mx]	threeam	Link
2024-02-01	[gatesshields.com]	lockbit3	Link
2024-02-01	[manchesterfertility.com]	lockbit3	Link
2024-02-01	[stemcor.com]	lockbit3	Link
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	Link
2024-02-01	[dms-imaging]	cuba	Link
2024-02-01	[bandcllp.com]	lockbit3	Link
2024-02-01	[taloninternational.com]	lockbit3	Link
2024-02-01	[Southwark Council]	meow	Link
2024-02-01	[Robert D. Clements Jr Law Group, LLLP]	bianlian	Link
2024-02-01	[CNPC Peru S.A.]	rhysida	Link
2024-02-01	[Primeimaging database for sale]	everest	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.