Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240320

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) . . . 7
3.3 Sicherheitslücken Meldungen von Tenable . . . 10

4 Aktiv ausgenutzte Sicherheitslücken **12**
4.1 Exploits der letzten 5 Tage . . . 12
4.2 0-Days der letzten 5 Tage . . . 16

5 Die Hacks der Woche **17**
5.0.1 Hättest du diese Lücke gefunden? . . . 17

6 Cyberangriffe: (Mär) **18**

7 Ransomware-Erpressungen: (Mär) **19**

8 Quellen **27**
8.1 Quellenverzeichnis . . . 27

9 Impressum **29**

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

Sicherheitsupdates für Firefox und Thunderbird

Mozilla dichtet zahlreiche Sicherheitslücken im Webbrowser Firefox und Mailer Thunderbird ab.

- Link

—

Spring Security: Zugriffskontrollmechanismen in Java-Framework kaputt

Die auf Sicherheitsmechanismen spezialisierte Unterbibliothek des Java-Entwicklungsframeworks kommt in manchen Fallen aus dem Tritt. Updates sind verfügbar.

- Link

—

Home- und Raspberry-Matic: Kritische Lücke erlaubt Codeschmuggel

In HomeMatic sowie in RaspberryMatic klafft eine Codeschmuggel-Lücke. Sie gilt als kritisch. Ein Update steht bereit.

- Link

—

Spring Framework: Updates beheben neue, alte Sicherheitslücke

Nutzen Spring-basierte Anwendungen eine URL-Parsing-Funktion des Frameworks, öffnen sie sich für verschiedene Attacken. Nicht zum ersten Mal.

- Link

—

HP: Viele Laptops und PCs von Codeschmuggel-Lücke betroffen

Eine BIOS-Sicherheitsfunktion von HP-Laptops und -PCs kann von Angreifern umgangen werden. BIOS-Updates stehen bereit oder werden grad entwickelt.

- Link

—

Cisco schließt hochriskante Lücken in IOS XR

Cisco warnt vor SIcherheitslücken mit teils hohem Risiko im Router-Betriebssystem IOS XR. Updates stehen bereit.

- Link

—

Fortinet-Patchday: Updates gegen kritische Schwachstellen

Fortinet hat zum März-Patchday Sicherheitslücken in FortiOS, FortiProxy, FortiClientEMS und im FortiManager öffentlich gemacht.

- Link

—

Adobe-Patchday: Angreifer können verwundbare Systeme übernehmen

Adobe stopft am März-Patchday teils kritische Sicherheitslücken in sechs Produkten. Sie erlauben unter anderem Codeschmuggel.

- Link

—

Microsoft Patchday: Hersteller stopft 59 Sicherheitslücken

Der März-Patchday von Microsoft ist etwas weniger umfangreich: 59 Sicherheitslecks haben die Entwickler gestopft.

- Link

—

Google Chrome: Lücke erlaubte Codeschmuggel

Google schließt drei Sicherheitslücken im Webbrowser Chrome. Mindestens eine gilt als hochriskant, Angreifer könnten Schadcode dadurch einschleusen.

- 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-2023-6895	0.901600000	0.987200000	Link
CVE-2023-6553	0.916210000	0.988350000	Link
CVE-2023-5360	0.967230000	0.996360000	Link
CVE-2023-4966	0.966110000	0.996040000	Link
CVE-2023-47246	0.943540000	0.991450000	Link
CVE-2023-46805	0.962740000	0.994950000	Link
CVE-2023-46747	0.972020000	0.998050000	Link
CVE-2023-46604	0.973060000	0.998610000	Link
CVE-2023-43177	0.927670000	0.989630000	Link
CVE-2023-42793	0.970930000	0.997590000	Link
CVE-2023-39143	0.933560000	0.990230000	Link
CVE-2023-38646	0.916640000	0.988410000	Link
CVE-2023-38205	0.934710000	0.990360000	Link
CVE-2023-38203	0.960070000	0.994380000	Link
CVE-2023-38035	0.972370000	0.998290000	Link
CVE-2023-36845	0.966580000	0.996150000	Link
CVE-2023-3519	0.911860000	0.988000000	Link
CVE-2023-35082	0.935540000	0.990450000	Link
CVE-2023-35078	0.963380000	0.995150000	Link
CVE-2023-34960	0.935410000	0.990440000	Link
CVE-2023-34634	0.925600000	0.989360000	Link
CVE-2023-34362	0.960450000	0.994490000	Link
CVE-2023-34039	0.901300000	0.987170000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3368	0.904650000	0.987400000	Link
CVE-2023-33246	0.973410000	0.998820000	Link
CVE-2023-32315	0.973840000	0.999060000	Link
CVE-2023-32235	0.905760000	0.987470000	Link
CVE-2023-30625	0.948330000	0.992170000	Link
CVE-2023-30013	0.945460000	0.991750000	Link
CVE-2023-29300	0.963690000	0.995250000	Link
CVE-2023-29298	0.921360000	0.988870000	Link
CVE-2023-28771	0.922340000	0.988980000	Link
CVE-2023-28432	0.941310000	0.991100000	Link
CVE-2023-28121	0.929770000	0.989770000	Link
CVE-2023-27524	0.972240000	0.998210000	Link
CVE-2023-27372	0.971520000	0.997860000	Link
CVE-2023-27350	0.971970000	0.998030000	Link
CVE-2023-26469	0.937680000	0.990690000	Link
CVE-2023-26360	0.962420000	0.994860000	Link
CVE-2023-26035	0.970030000	0.997220000	Link
CVE-2023-25717	0.957880000	0.993860000	Link
CVE-2023-2479	0.962540000	0.994900000	Link
CVE-2023-24489	0.973400000	0.998820000	Link
CVE-2023-23752	0.948570000	0.992210000	Link
CVE-2023-23397	0.917330000	0.988480000	Link
CVE-2023-23333	0.963260000	0.995120000	Link
CVE-2023-22527	0.965680000	0.995930000	Link
CVE-2023-22518	0.970110000	0.997250000	Link
CVE-2023-22515	0.971880000	0.998000000	Link
CVE-2023-21839	0.960490000	0.994500000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21554	0.959700000	0.994260000	Link
CVE-2023-20887	0.965070000	0.995690000	Link
CVE-2023-20198	0.919220000	0.988670000	Link
CVE-2023-1671	0.961560000	0.994680000	Link
CVE-2023-0669	0.968640000	0.996790000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 19 Mar 2024

[NEU] [hoch] IBM App Connect Enterprise: Schwachstelle ermöglicht Codeausführung und Offenlegung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM App Connect Enterprise ausnutzen, um beliebigen Programmcode auszuführen und Informationen offenzulegen.

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] Liferay Portal und DXP: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Liferay Liferay DXP und Liferay Liferay Portal ausnutzen, um Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern.

- Link

—

Tue, 19 Mar 2024

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

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

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu

umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 19 Mar 2024

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

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um Informationen offenzulegen.

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ruby ausnutzen, um Dateien zu manipulieren.

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Denial of Service

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- Link

—

Tue, 19 Mar 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] Cacti: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Tue, 19 Mar 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

—

Tue, 19 Mar 2024

[UPDATE] [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

—

Tue, 19 Mar 2024

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

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

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- Link

—

Tue, 19 Mar 2024

[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- Link

—

Tue, 19 Mar 2024

[NEU] [hoch] VMware Tanzu Spring Security: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 18 Mar 2024

[UPDATE] [hoch] libTIFF: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode mit Benutzerrechten

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in libTIFF ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen oder um einen Denial of Service Zustand

herbeizuführen.

- Link

—

Mon, 18 Mar 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux und Oracle Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 18 Mar 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Mon, 18 Mar 2024

[UPDATE] [hoch] IBM Business Automation Workflow: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in IBM Business Automation Workflow ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 18 Mar 2024

[UPDATE] [hoch] Microsoft Visual Studio 2022: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um einen Denial of Service Angriff durchzuführen oder seine Privilegien zu erweitern.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/19/2024	[Arcserve UDP Console Authentication Bypass (CVE-2024-0799)]	critical
3/19/2024	[Google Chrome < 123.0.6312.58 Multiple Vulnerabilities]	critical
3/19/2024	[Amazon Linux AMI : ImageMagick (ALAS-2024-1926)]	critical
3/19/2024	[RHEL 8 : emacs (RHSA-2024:1408)]	critical
3/20/2024	[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel (AWS) vulnerabilities (USN-6681-4)]	high
3/20/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (Oracle) vulnerabilities (USN-6686-3)]	high
3/20/2024	[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6702-1)]	high
3/20/2024	[Ubuntu 22.04 LTS / 23.10 : Linux kernel (AWS) vulnerabilities (USN-6680-3)]	high
3/19/2024	[Mozilla Thunderbird < 115.9]	high
3/19/2024	[Mozilla Thunderbird < 115.9]	high
3/19/2024	[Cisco IOS Software Command Authorization Bypass (cisco-sa-aaascp-Tyj4fEJm)]	high
3/19/2024	[Cisco IOS XE Software Command Authorization Bypass (cisco-sa-aaascp-Tyj4fEJm)]	high
3/19/2024	[RHEL 8 : kpatch-patch (RHSA-2024:1377)]	high
3/19/2024	[RHEL 8 : squid:4 (RHSA-2024:1375)]	high
3/19/2024	[RHEL 8 : kernel-rt (RHSA-2024:1382)]	high
3/19/2024	[RHEL 9 : squid (RHSA-2024:1376)]	high
3/19/2024	[Slackware Linux 15.0 / current gnutls Multiple Vulnerabilities (SSA:2024-079-01)]	high
3/19/2024	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2024-079-03)]	high
3/19/2024	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2024-079-02)]	high
3/19/2024	[Debian dsa-5641 : fontforge - security update]	high

Datum	Schwachstelle	Bewertung
3/19/2024	[RHEL 8 : edk2 (RHSA-2024:1415)]	high
3/19/2024	[RHEL 9 : libreoffice (RHSA-2024:1423)]	high
3/19/2024	[RHEL 8 : postgresql (RHSA-2024:1428)]	high
3/19/2024	[RHEL 8 : postgresql (RHSA-2024:1429)]	high
3/19/2024	[RHEL 8 : kernel (RHSA-2024:1404)]	high
3/19/2024	[RHEL 8 : gmp update (Moderate) (RHSA-2024:1412)]	high
3/19/2024	[RHEL 8 : cups (RHSA-2024:1409)]	high
3/19/2024	[RHEL 8 : postgresql (RHSA-2024:1422)]	high
3/19/2024	[RHEL 8 : bind (RHSA-2024:1406)]	high
3/19/2024	[RHEL 9 : libreoffice (RHSA-2024:1425)]	high
3/19/2024	[RHEL 8 : postgresql (RHSA-2024:1426)]	high
3/19/2024	[RHEL 9 : libreoffice (RHSA-2024:1427)]	high
3/19/2024	[RHEL 8 : libX11 (RHSA-2024:1417)]	high
3/19/2024	[RHEL 8 : ruby:3.1 (RHSA-2024:1431)]	high
3/19/2024	[RHEL 9 : nodejs (RHSA-2024:1424)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 19 Mar 2024

Tramyardg Autoexpress 1.3.0 Cross Site Scripting

Tramyardg Autoexpress version 1.3.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 19 Mar 2024

Tramyardg Autoexpress 1.3.0 Authentication Bypass

Tramyardg Autoexpress version 1.3.0 allows for authentication bypass via unauthenticated API access to admin functionality. This could allow a remote anonymous attacker to delete or update vehicles as well as upload images for vehicles.

- Link

—

” “Tue, 19 Mar 2024

Tramyardg Autoexpress 1.3.0 SQL Injection

Tramyardg Autoexpress version 1.3.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 19 Mar 2024

SurveyJS Survey Creator 1.9.132 Cross Site Scripting

SurveyJS Survey Creator versions 1.9.132 and below suffer from both reflective and persistent cross site scripting vulnerabilities.

- Link

—

” “Tue, 19 Mar 2024

Quick.CMS 6.7 SQL Injection

Quick.CMS version 6.7 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 19 Mar 2024

Atlassian Confluence 8.5.3 Remote Code Execution

Atlassian Confluence versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0 through 8.5.3 suffer from a remote code execution vulnerability.

- Link

—

” “Tue, 19 Mar 2024

Backdrop CMS 1.23.0 Cross Site Scripting

Backdrop CMS version 1.23.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 19 Mar 2024

ZoneMinder Snapshots Remote Code Execution

ZoneMinder Snapshots versions prior to 1.37.33 suffer from an unauthenticated remote code execution vulnerability.

- Link

—

” “Tue, 19 Mar 2024

WEBIGniter 28.7.23 Cross Site Scripting

WEBIGniter version 28.7.23 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 19 Mar 2024

WordPress File Upload Cross Site Scripting

WordPress File Upload plugin versions prior to 4.23.3 suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 19 Mar 2024

Gibbon LMS 26.0.00 PHP Deserialization / Code Execution

Gibbon LMS version 26.0.00 suffers from a PHP deserialization vulnerability that allows for authenticated remote code execution.

- Link

—

” “Tue, 19 Mar 2024

Fortra FileCatalyst Workflow 5.x Remote Code Execution

This is a proof of concept exploit for CVE-2024-25153, a remote code execution vulnerability in Fortra FileCatalyst Workflow versions 5.x, before 5.1.6 Build 114.

- Link

—

” “Tue, 19 Mar 2024

Generic And Automated Drive-By GPU Cache Attacks From The Browser

In this paper, the authors present the first GPU cache side-channel attack from within the browser, more specifically from the restricted WebGPU environment. The foundation for our generic and automated attacks are self-configuring primitives applicable to a wide variety of devices, which they demonstrate on a set of 11 desktop GPUs from 5 different generations and 2 vendors.

- Link

—

” “Mon, 18 Mar 2024

dav1d Integer Overflow / Out-Of-Bounds Write

There is an integer overflow in dav1d when decoding an AV1 video with large width/height. The integer overflow may result in an out-of-bounds write.

- Link

—

” “Mon, 18 Mar 2024

UPS Network Management Card 4 Path Traversal

UPS Network Management Card version 4 suffers from a path traversal vulnerability.

- Link

—

” “Mon, 18 Mar 2024

Gasmark Pro 1.0 Shell Upload

Gasmark Pro version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 18 Mar 2024

Nokia BMC Log Scanner 13 Command Injection

Nokia BMC Log Scanner version 13 suffers from a remote command injection vulnerability.

- Link

—

” “Mon, 18 Mar 2024

vm2 3.9.19 Sandbox Escape

vm2 versions 3.9.19 and below suffer from a sandbox escape vulnerability.

- Link

—

” “Fri, 15 Mar 2024

Financials By Coda Authorization Bypass

Financials by Coda versions prior to 2023Q4 suffer from an incorrect access control authorization bypass vulnerability. The Change Password feature can be abused in order to modify the password of any user of the application.

- Link

—

” “Fri, 15 Mar 2024

Financials By Coda Cross Site Scripting

Financials by Coda versions prior to 2023Q4 suffer from a cross site scripting vulnerability.

- Link

—

” “Fri, 15 Mar 2024

HALO 2.13.1 CORS Issue

HALO version 2.13.1 has an insecure cross-origin resource sharing setting that allows an arbitrary origin.

- Link

—

” “Fri, 15 Mar 2024

Membership Management System 1.0 SQL Injection / Shell Upload

Membership Management System version 1.0 suffers from remote shell upload and remote SQL injec-

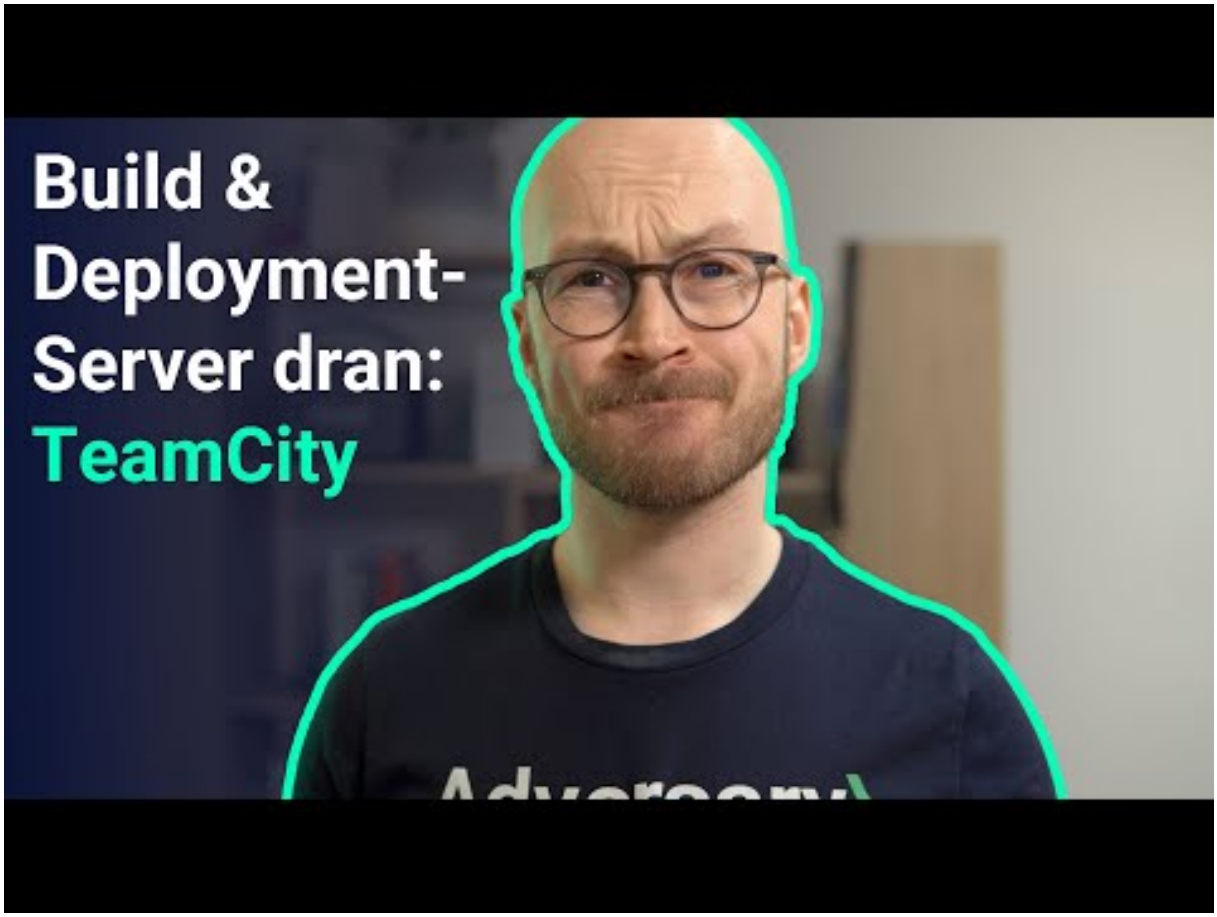
tion vulnerabilities.
- Link
—
” “Thu, 14 Mar 2024
Checkmk Agent 2.0.0 / 2.1.0 / 2.2.0 Local Privilege Escalation
Checkmk Agent versions 2.0.0, 2.1.0, and 2.2.0 suffer from a local privilege escalation vulnerability.
- Link
—
” “Thu, 14 Mar 2024
Vinchin Backup And Recovery 7.2 Command Injection
Vinchin Backup and Recovery versions 7.2 and below suffer from an authentication command injection vulnerability.
- Link
—
” “Thu, 14 Mar 2024
Fortinet FortiOS Out-Of-Bounds Write
Fortinet FortiOS suffers from an out of bounds write vulnerability. Affected includes Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, and 1.0.0 through 1.0.7.
- Link
—
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Hättest du diese Lücke gefunden?



Zum Youtube Video

6 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2024-03-17	Ville de Pensacola	[USA]	Link
2024-03-17	South China Athletic Association	[HKG]	Link
2024-03-15	Fujitsu	[JPN]	Link
2024-03-15	Deutsches Meeresmuseum de Stralsund	[DEU]	Link
2024-03-14	NHS Dumfries and Galloway	[GBR]	Link
2024-03-14	Scranton School District	[USA]	Link
2024-03-13	Maxis	[MYS]	Link
2024-03-12	Riverview School District	[USA]	Link
2024-03-11	District de North Vancouver	[CAN]	Link
2024-03-10	edpnet	[BEL]	Link
2024-03-10	Town of Huntsville	[CAN]	Link
2024-03-10	MarineMax	[USA]	Link
2024-03-10	EDIS	[AUT]	Link
2024-03-09	Leicester City Council	[GBR]	Link
2024-03-08	Kärntner Landesversicherung (KLV)	[AUT]	Link
2024-03-07	Administradora de Subsidios Sociales (ADESS)	[DOM]	Link
2024-03-07	Beyers Koffie	[BEL]	Link
2024-03-06	Brasserie Duvel Moortgat	[BEL]	Link
2024-03-06	Nisqually Red Wind Casino	[USA]	Link
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	Link
2024-03-04	South St. Paul Public Schools	[USA]	Link
2024-03-01	Hansab	[EST]	Link

7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-20	[South Star Electronics]	trigona	Link
2024-03-19	[Accipiter Capital Management, LLC]	medusa	Link
2024-03-19	[Urban Strategies]	medusa	Link
2024-03-19	[Sting AD]	hunters	Link
2024-03-19	[Jasper-Dubois County Public Library]	dragonforce	Link
2024-03-19	[Therapeutic Health Services]	hunters	Link
2024-03-19	[Panzeri Cattaneo]	hunters	Link
2024-03-19	[Retirement Line]	snatch	Link
2024-03-19	[Delta Pipeline]	bianlian	Link
2024-03-19	[Mayer Antonellis Jachowicz & Haranas, LLP]	bianlian	Link
2024-03-19	[P&B Capital Group]	bianlian	Link
2024-03-17	[Butler, Lavanceau & Sober]	snatch	Link
2024-03-18	[Dr. Leeman ENT]	bianlian	Link
2024-03-18	[HSI]	hunters	Link
2024-03-18	[AGL]	hunters	Link
2024-03-18	[Sun Holdings]	hunters	Link
2024-03-17	[paginesi]	stormous	Link
2024-03-18	[eclinicalsol.com]	cactus	Link
2024-03-18	[grupatopex.com]	cactus	Link
2024-03-18	[activeconceptsllc.com]	blackbasta	Link
2024-03-17	[Romark Laboratories]	medusa	Link
2024-03-18	[crinetics.com]	lockbit3	Link
2024-03-03	[highfashion.com.hk]	mallox	Link
2024-03-14	[Ramdev Chemical Industries]	mallox	Link
2024-03-16	[Rafum Group]	mallox	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-16	[Autorità di Sistema Portuale del Mar Tirreno Settentrionale It]	medusa	Link
2024-03-16	[Elior UK]	medusa	Link
2024-03-16	[Indoarsip]	trigona	Link
2024-03-16	[Bwizer]	trigona	Link
2024-03-16	[Topa Partners]	trigona	Link
2024-03-16	[HUDSONBUSSALES.COM]	clop	Link
2024-03-15	[Desco Steel]	medusa	Link
2024-03-15	[Metzger Veterinary Services]	medusa	Link
2024-03-16	[Consolidated Benefits Resources]	bianlian	Link
2024-03-16	[agribank.com.na]	lockbit3	Link
2024-03-16	[triella.com]	lockbit3	Link
2024-03-16	[rrib.com]	lockbit3	Link
2024-03-16	[newmans-online.co.uk]	lockbit3	Link
2024-03-16	[hdstrading.com]	lockbit3	Link
2024-03-16	[duttonbrock.com]	lockbit3	Link
2024-03-16	[colefabrics.com]	lockbit3	Link
2024-03-16	[bergmeister.eu]	lockbit3	Link
2024-03-16	[automotionshade.com]	lockbit3	Link
2024-03-16	[Miki Travel]	hunters	Link
2024-03-16	[certifiedcollection.com]	lockbit3	Link
2024-03-16	[Acculabs Inc]	incransom	Link
2024-03-08	[oyaksgs.com.tr]	lockbit3	Link
2024-03-15	[elezabypharmacy.com]	lockbit3	Link
2024-03-15	[South St Paul Public Schools]	blacksuit	Link
2024-03-12	[ATL Leasing]	hunters	Link
2024-03-14	[lostlb]	stormous	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-14	[education.eeb-lost]	stormous	Link
2024-03-14	[worthenind.com]	lockbit3	Link
2024-03-14	[rushenergyservices.com]	lockbit3	Link
2024-03-14	[sbmandco.com]	lockbit3	Link
2024-03-14	[mckimcreed.com]	lockbit3	Link
2024-03-14	[moperry.com]	lockbit3	Link
2024-03-14	[Cosmocolor]	hunters	Link
2024-03-14	[voidinteractive.net you are welcome in our chat]	donutleaks	Link
2024-03-14	[journeyfreight.com]	lockbit3	Link
2024-03-14	[dhanisisd.net]	lockbit3	Link
2024-03-14	[mioa.gov]	stormous	Link
2024-03-14	[gfad.de]	blackbasta	Link
2024-03-14	[Keboda Technology Co., Ltd.]	bianlian	Link
2024-03-14	[iamdesign.com]	abyss	Link
2024-03-14	[yarco.com]	abyss	Link
2024-03-13	[McKim & Creed]	ransomhub	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Summit Almonds]	akira	Link
2024-03-13	[Encina Wastewater Authority]	blackbyte	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Felda Global Ventures Holdings Berhad]	qilin	Link
2024-03-13	[geruestbau.com]	lockbit3	Link
2024-03-13	[Judge Rotenberg Center]	blacksuit	Link
2024-03-12	[Dörr Group]	snatch	Link
2024-03-13	[Kovra]	ransomhub	Link
2024-03-13	[Brewer Davidson]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-13	[Forstinger Österreich GmbH]	8base	Link
2024-03-04	[vsexshop.ru]	werewolves	Link
2024-03-11	[QEO Group]	play	Link
2024-03-12	[ATL]	hunters	Link
2024-03-12	[duvel.com	boulevard.com]	blackbasta
2024-03-11	[Kenneth Young Center]	medusa	Link
2024-03-12	[sunholdings.net]	lockbit3	Link
2024-03-12	[xcelbrands.com]	blackbasta	Link
2024-03-12	[cpacsystems.se]	blackbasta	Link
2024-03-12	[elmatic.de]	blackbasta	Link
2024-03-12	[keystonetech.com]	blackbasta	Link
2024-03-12	[dutyfreeamericas.com]	blackbasta	Link
2024-03-12	[sierralobo.com]	blackbasta	Link
2024-03-12	[contechs.co.uk]	blackbasta	Link
2024-03-12	[creativeenvironments.com]	blackbasta	Link
2024-03-12	[linksunlimited.com]	blackbasta	Link
2024-03-12	[imperialtrading.com]	blackbasta	Link
2024-03-12	[Brooks Tropicals]	rhysida	Link
2024-03-12	[Withall]	blacksuit	Link
2024-03-12	[WALKERSANDFORD]	blacksuit	Link
2024-03-12	[Kaplan]	hunters	Link
2024-03-06	[Sprimoglass]	8base	Link
2024-03-11	[Schokinag]	play	Link
2024-03-11	[Zips Car Wash]	play	Link
2024-03-11	[Bechtold]	play	Link
2024-03-11	[Canada Revenue Agency]	play	Link
2024-03-11	[White Oak Partners]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-11	[Ruda Auto]	play	Link
2024-03-11	[Image Pointe]	play	Link
2024-03-11	[Grassmid Transport]	play	Link
2024-03-11	[Fashion UK]	play	Link
2024-03-11	[QI Group]	play	Link
2024-03-11	[BiTec]	play	Link
2024-03-11	[Bridger Insurance]	play	Link
2024-03-11	[SREE Hotels]	play	Link
2024-03-11	[Q?? ??o??]	play	Link
2024-03-11	[Premier Technology]	play	Link
2024-03-11	[londonvisionclinic.com]	lockbit3	Link
2024-03-11	[lec-london.uk]	lockbit3	Link
2024-03-11	[Computan]	ransomhub	Link
2024-03-11	[plymouth.com]	cactus	Link
2024-03-11	[neigc.com]	abyss	Link
2024-03-11	[gpaa.gov.za]	lockbit3	Link
2024-03-11	[NetVigour]	hunters	Link
2024-03-11	[cleshar.co.uk]	cactus	Link
2024-03-11	[ammega.com]	cactus	Link
2024-03-11	[renypicot.es]	cactus	Link
2024-03-11	[Scadea Solutions]	ransomhub	Link
2024-03-09	[https://www.consorzioinnova.it]	alphalocker	Link
2024-03-09	[DVT]	ransomhub	Link
2024-03-09	[Rekamy]	ransomhub	Link
2024-03-09	[go4kora]	ransomhub	Link
2024-03-09	[H + G EDV Vertriebs]	blacksuit	Link
2024-03-09	[Fincasrevuelta]	everest	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-09	[Lindsay Municipal Hospital]	bianlian	Link
2024-03-09	[Group Health Cooperative - Rev 500kk]	blacksuit	Link
2024-03-09	[ACE Air Cargo]	hunters	Link
2024-03-09	[Watsonclinic.com]	donutleaks	Link
2024-03-06	[Continental Aerospace Technologies]	play	Link
2024-03-08	[redwoodcoastrc.org]	lockbit3	Link
2024-03-08	[PowerRail Distribution]	blacksuit	Link
2024-03-08	[Denninger’s]	medusa	Link
2024-03-08	[SIEA]	ransomhub	Link
2024-03-08	[Hozzify]	ransomhub	Link
2024-03-07	[rmhfranchise.com]	lockbit3	Link
2024-03-07	[New York Home Healthcare]	bianlian	Link
2024-03-07	[Palmer Construction Co., Inc]	bianlian	Link
2024-03-07	[en-act-architecture]	qilin	Link
2024-03-07	[Merchant ID]	ransomhub	Link
2024-03-07	[SP Mundi]	ransomhub	Link
2024-03-07	[www.duvel.com]	stormous	Link
2024-03-06	[www.loghmanpharma.com]	stormous	Link
2024-03-06	[MainVest]	play	Link
2024-03-06	[C?????????? A???????e T???????????]	play	Link
2024-03-05	[Haivision MCS]	medusa	Link
2024-03-06	[Tocci Building Corporation]	medusa	Link
2024-03-06	[JVCKENWOOD]	medusa	Link
2024-03-06	[American Renal Associates]	medusa	Link
2024-03-06	[US #1364 Federal Credit Union]	medusa	Link
2024-03-06	[viadirectamarketing]	stormous	Link
2024-03-06	[Liquid Environmental Solutions]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-06	[Infosoft]	akira	Link
2024-03-06	[brightwires.com.sa]	qilin	Link
2024-03-06	[Medical Billing Specialists]	akira	Link
2024-03-06	[Telecentro]	akira	Link
2024-03-06	[Steiner (Austrian furniture makers)]	akira	Link
2024-03-06	[Biomedical Research Institute]	meow	Link
2024-03-06	[K???o???]	play	Link
2024-03-06	[Kudulis Reisinger Price]	8base	Link
2024-03-06	[Global Zone]	8base	Link
2024-03-06	[Mediplast AB]	8base	Link
2024-03-05	[airbogo]	stormous	Link
2024-03-05	[sunwave.com.cn]	lockbit3	Link
2024-03-05	[SJCME.EDU]	clop	Link
2024-03-05	[central.k12.or.us]	lockbit3	Link
2024-03-05	[iemsc.com]	qilin	Link
2024-03-05	[hawita-gruppe]	qilin	Link
2024-03-05	[Future Generations Foundation]	meow	Link
2024-03-04	[Seven Seas Group]	snatch	Link
2024-03-04	[Paul Davis Restoration]	medusa	Link
2024-03-04	[Veeco]	medusa	Link
2024-03-04	[dismogas]	stormous	Link
2024-03-04	[everplast]	stormous	Link
2024-03-04	[DiVal Safety Equipment, Inc.]	hunters	Link
2024-03-04	[America Chung Nam orACN]	akira	Link
2024-03-03	[jovani.com]	lockbit3	Link
2024-03-03	[valoremreply.com]	lockbit3	Link
2024-03-04	[Martin’s, Inc.]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-03	[Prompt Financial Solutions]	medusa	Link
2024-03-03	[Sophiahemmet University]	medusa	Link
2024-03-03	[Centennial Law Group LLP]	medusa	Link
2024-03-03	[Eastern Rio Blanco Metropolitan]	medusa	Link
2024-03-03	[Chris Argiropoulos Professional]	medusa	Link
2024-03-03	[THAISUMMIT.US]	clop	Link
2024-03-03	[THESAFIRCHOICE.COM]	clop	Link
2024-03-03	[ipmaltamira]	alphv	Link
2024-03-03	[earnesthealth.com]	lockbit3	Link
2024-03-03	[Ward Transport & Logistics]	dragonforce	Link
2024-03-03	[Ponoka.ca]	cloak	Link
2024-03-03	[stockdevelopment.com]	lockbit3	Link
2024-03-03	[Ewig Usa]	alphv	Link
2024-03-02	[aerospace.com]	lockbit3	Link
2024-03-02	[starkpower.de]	lockbit3	Link
2024-03-02	[roehr-stolberg.de]	lockbit3	Link
2024-03-02	[schuett-grundei.de]	lockbit3	Link
2024-03-02	[unitednotions.com]	lockbit3	Link
2024-03-02	[smuldes.com]	lockbit3	Link
2024-03-02	[esser-ps.de]	lockbit3	Link
2024-03-01	[SBM & Co [You have 48 hours. Check your e-mail]]	alphv	Link
2024-03-01	[Skyland Grain]	play	Link
2024-03-01	[American Nuts]	play	Link
2024-03-01	[A&A Wireless]	play	Link
2024-03-01	[Powill Manufacturing & Engineering]	play	Link
2024-03-01	[Trans+Plus Systems]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-01	[Hedlunds]	play	Link
2024-03-01	[Red River Title]	play	Link
2024-03-01	[Compact Mould]	play	Link
2024-03-01	[Winona Pattern & Mold]	play	Link
2024-03-01	[Marketon]	play	Link
2024-03-01	[Stack Infrastructure]	play	Link
2024-03-01	[Coastal Car]	play	Link
2024-03-01	[New Bedford Welding Supply]	play	Link
2024-03-01	[Influence Communication]	play	Link
2024-03-01	[Kool-air]	play	Link
2024-03-01	[FBi Construction]	play	Link
2024-03-01	[SBM & Co]	alphv	Link
2024-03-01	[Shooting House]	ransomhub	Link
2024-03-01	[Crystal Window & Door Systems]	dragonforce	Link
2024-03-01	[Gilmore Construction]	blacksuit	Link
2024-03-01	[Petrus Resources Ltd]	alphv	Link
2024-03-01	[CoreData]	akira	Link
2024-03-01	[Gansevoort Hotel Group]	akira	Link
2024-03-01	[DJI Company]	mogilevich	Link
2024-03-01	[Kick]	mogilevich	Link
2024-03-01	[Shein]	mogilevich	Link
2024-03-01	[Kumagai Gumi Group]	alphv	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.