
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240212



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	21
5.0.1 AnyDesk-Hack und Jenkins-Lücke	21
6 Cyberangriffe: (Feb)	22
7 Ransomware-Erpressungen: (Feb)	22
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

Elastic Stack: Pufferüberlauf ermöglicht Codeschmuggel in Kibana-Komponente

Der in Kibana integrierte Chromium-Browser verursachte das Problem nur auf bestimmten Plattformen. Updates und eine Übergangslösung stehen bereit.

- [Link](#)

—

Bootloader-Lücke: Viele Linux-Distributionen sind gefährdet

Im Bootloader shim, der Secure-Boot auch für nicht-Windows-Betriebssysteme erlaubt, klafft eine Sicherheitslücke.

- [Link](#)

—

Sicherheitsupdates: Authentifizierung von Ivanti Connect Secure & Co. defekt

Angreifer können ohne Anmeldung auf Ivanti Connect Secure, Policy Secure und ZTA Gateway zugreifen.

- [Link](#)

—

SonicOS SSL-VPN: Angreifer können Authentifizierung umgehen

Sonicwall warnt vor einer Sicherheitslücke im SonicOS SSL-VPN, durch die Angreifer die Authentifizierung umgehen können.

- [Link](#)

—

Sicherheitsupdates: SSL-VPN-Komponente von FortiOS angreifbar

Wichtige Sicherheitspatches schließen kritische Lücken in FortiOS und FortiSIEM. Admins sollten zügig handeln.

- [Link](#)

—

Samsung Magician: Update stopft Sicherheitsleck im SSD-Tool

Samsung bietet mit Magician eine Software zum Verwalten von SSDs, Speichersticks und -Karten des Herstellers. Ein Update schließt eine Lücke darin.

- [Link](#)

—

Sicherheitslücken: Codeschmuggel und Leistungsverweigerung bei ClamAV

Der Parser für das OLE2-Dateiformat enthält einen Pufferüberlauf und mit speziell präparierten Dateinamen lassen sich offenbar eigene Befehlszeilen ausführen.

- [Link](#)

Update gegen Sicherheitsleck in Alpha Innotec- und Novelan-Wärmepumpen

Der Hersteller der Alpha Innotec- und Novelan-Wärmepumpen erläutert, wie Besitzer an Updates zum Schließen der Passwort-Schwachstelle kommen.

- [Link](#)

Sicherheitsupdates: Kritische Lücken bedrohen Cisco Expressway Series

Der Netzwerkausrüster Cisco hat seine Kollaborationssoftware Expressway Series abgesichert. Außerdem haben sie die ClamAV-Komponente gepatcht.

- [Link](#)

Rechtausweitung durch Lücken in Veeam Recovery Orchestrator möglich

Veeam flickt die Recovery Orchestrator-Software. Sicherheitslücken darin erlauben böartigen Akteuren die Ausweitung von Rechten.

- [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	0.987390000	Link
CVE-2023-5360	0.967230000	0.996220000	Link
CVE-2023-4966	0.964760000	0.995320000	Link
CVE-2023-47246	0.941910000	0.990880000	Link
CVE-2023-46805	0.962740000	0.994730000	Link
CVE-2023-46747	0.971390000	0.997660000	Link
CVE-2023-46604	0.972850000	0.998390000	Link
CVE-2023-43177	0.932620000	0.989850000	Link
CVE-2023-42793	0.973130000	0.998570000	Link
CVE-2023-41265	0.915100000	0.987930000	Link
CVE-2023-39143	0.920480000	0.988500000	Link
CVE-2023-38205	0.932790000	0.989880000	Link
CVE-2023-38035	0.974110000	0.999210000	Link
CVE-2023-36845	0.964780000	0.995330000	Link
CVE-2023-3519	0.912410000	0.987730000	Link
CVE-2023-35082	0.962080000	0.994570000	Link
CVE-2023-35078	0.952060000	0.992490000	Link
CVE-2023-34960	0.931300000	0.989670000	Link
CVE-2023-34634	0.919000000	0.988340000	Link
CVE-2023-34362	0.960730000	0.994270000	Link
CVE-2023-3368	0.928930000	0.989390000	Link
CVE-2023-33246	0.973540000	0.998790000	Link
CVE-2023-32315	0.973860000	0.999010000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32235	0.902020000	0.986880000	Link
CVE-2023-30625	0.950540000	0.992190000	Link
CVE-2023-30013	0.936180000	0.990160000	Link
CVE-2023-29300	0.958470000	0.993750000	Link
CVE-2023-28771	0.923800000	0.988890000	Link
CVE-2023-28121	0.932010000	0.989720000	Link
CVE-2023-27524	0.972220000	0.998100000	Link
CVE-2023-27372	0.970420000	0.997250000	Link
CVE-2023-27350	0.972270000	0.998140000	Link
CVE-2023-26469	0.936750000	0.990250000	Link
CVE-2023-26360	0.957020000	0.993470000	Link
CVE-2023-26035	0.968710000	0.996700000	Link
CVE-2023-25717	0.962730000	0.994720000	Link
CVE-2023-25194	0.916080000	0.988040000	Link
CVE-2023-2479	0.964780000	0.995330000	Link
CVE-2023-24489	0.973640000	0.998850000	Link
CVE-2023-23752	0.949820000	0.992100000	Link
CVE-2023-23397	0.906590000	0.987160000	Link
CVE-2023-22527	0.974310000	0.999350000	Link
CVE-2023-22518	0.970760000	0.997360000	Link
CVE-2023-22515	0.962730000	0.994720000	Link
CVE-2023-21839	0.961800000	0.994500000	Link
CVE-2023-21554	0.961220000	0.994350000	Link
CVE-2023-20887	0.965640000	0.995710000	Link
CVE-2023-20198	0.919220000	0.988360000	Link
CVE-2023-1671	0.964220000	0.995200000	Link
CVE-2023-0669	0.968670000	0.996670000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 09 Feb 2024

[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 09 Feb 2024

[UPDATE] [hoch] Xen: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Xen ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 09 Feb 2024

[NEU] [kritisch] Fortinet FortiOS: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Fortinet FortiOS ausnutzen, um beliebigen Code auszuführen.

- [Link](#)

—

Fri, 09 Feb 2024

[NEU] [hoch] Red Hat Enterprise Linux (Pillow): Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente "Pillow" ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 09 Feb 2024

[NEU] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

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

- [Link](#)

—

Fri, 09 Feb 2024

[NEU] [hoch] Red Hat Enterprise Linux (unbound): Schwachstelle ermöglicht nicht spezifizierten

Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente "unbound" ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

Fri, 09 Feb 2024

[NEU] [hoch] Rancher: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Rancher ausnutzen, um Informationen offenzulegen, XSS-Angriffe durchzuführen oder seine Privilegien zu erweitern.

- [Link](#)

Fri, 09 Feb 2024

[UPDATE] [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](#)

Fri, 09 Feb 2024

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

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

- [Link](#)

Fri, 09 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](#)

Fri, 09 Feb 2024

[UPDATE] [hoch] Unify OpenScape Voice: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Unify OpenScape Voice ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

Fri, 09 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](#)

—

Fri, 09 Feb 2024

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

Ein entfernter, authentifzierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 09 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.

- [Link](#)

—

Fri, 09 Feb 2024

[UPDATE] [hoch] Fortinet FortiSIEM: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Fortinet FortiSIEM ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 09 Feb 2024

[UPDATE] [hoch] ClamAV: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in ClamAV ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

—

Fri, 09 Feb 2024

[NEU] [hoch] Linux "Shim": Schwachstelle ermöglicht Übernahme der Kontrolle

Ein anonymer Angreifer aus dem angrenzenden Netzwerk kann eine Schwachstelle in der "Shim" Komponente von Linux-Systemen ausnutzen, um die Kontrolle über ein betroffenes System zu übernehmen.

- [Link](#)

—

Fri, 09 Feb 2024

[NEU] [hoch] Ivanti Connect Secure and Ivanti Policy Secure: Schwachstelle ermöglicht Umgehung von Sicherheitsmechanismen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ivanti Connect Secure und Ivanti Policy Secure ausnutzen, um Sicherheitsmechanismen zu umgehen.

- [Link](#)

—
Thu, 08 Feb 2024

[NEU] [hoch] NetApp ActiveIQ Unified Manager: Schwachstelle ermöglicht Manipulation, Offenlegung und Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in NetApp ActiveIQ Unified Manager ausnutzen, um Daten zu manipulieren, Informationen offenzulegen oder einen Denial of Service zu verursachen.

- [Link](#)

—
Thu, 08 Feb 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Liferay Liferay Portal und Liferay Liferay DXP ausnutzen, um Informationen offenzulegen, Cross-Site-Scripting (XSS)-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder Dateien zu manipulieren.

- [Link](#)

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/9/2024	[TeamCity Server < 2023.11.3 Multiple Vulnerabilities]	critical
2/9/2024	[Cisco Expressway Series XSRF (cisco-sa-expressway-csrf-KnnZDMj3)]	critical
2/9/2024	[Ivanti Policy Secure 9.x / 22.x Multiple Vulnerabilities]	critical
2/9/2024	[Ivanti Avalanche < 6.4.2 Multiple Vulnerabilities]	critical
2/11/2024	[Fedora 38 : openssh (2024-2aac54ebb7)]	critical

Datum	Schwachstelle	Bewertung
2/10/2024	[Fedora 39 : firecracker / libkrum / rust-event-manager / rust-kvm-bindings / etc (2024-04877592b7)]	critical
2/9/2024	[ClamAV 0.104.x, 0.105.x, 1.0.0 < 1.0.4, 1.1.x, 1.2.0 < 1.2.1 RCE]	high
2/9/2024	[ClamAV 1.0.0 < 1.0.4, 1.1.x, 1.2.0 < 1.2.1 DoS]	high
2/9/2024	[AlmaLinux 8 : container-tools:rhel8 (ALSA-2024:0752)]	high
2/9/2024	[AlmaLinux 8 : container-tools:4.0 (ALSA-2024:0748)]	high
2/9/2024	[QNAP Photo Station OS Command Injection (QSA-24-08)]	high
2/9/2024	[PuTTY < 0.76 Insufficient Verification of Data Authenticity]	high
2/9/2024	[QNAP QTS / QuTS hero Multiple Vulnerabilities in QTS, QuTS hero, and QuTScld (QSA-24-05)]	high
2/9/2024	[Docker Desktop < 4.27.1 Multiple Vulnerabilities]	high
2/9/2024	[Docker Desktop < 4.27.1 Multiple Vulnerabilities]	high
2/9/2024	[Docker Desktop < 4.27.1 Multiple Vulnerabilities]	high
2/9/2024	[Ubuntu 22.04 LTS : Linux kernel (Intel IoTG) vulnerabilities (USN-6628-1)]	high
2/9/2024	[DLink DIR-610 Multiple Vulnerabilities]	high
2/9/2024	[IBM Java 7.1 < 7.1.5.21 / 8.0 < 8.0.8.20 Multiple Vulnerabilities]	high
2/9/2024	[FreeBSD : chromium – multiple security fixes (19047673-c680-11ee-86bb-a8a1599412c6)]	high
2/9/2024	[FreeBSD : Libgit2 – multiple vulnerabilities (43768ff3-c683-11ee-97d0-001b217b3468)]	high
2/9/2024	[FreeBSD : Composer – Code execution and possible privilege escalation (33ba2241-c68e-11ee-9ef3-001999f8d30b)]	high
2/9/2024	[FreeBSD : postgresql-server – non-owner REFRESH MATERIALIZED VIEW CONCURRENTLY executes arbitrary SQL (19e6dd1b-c6a5-11ee-9cd0-6cc21735f730)]	high
2/9/2024	[Oracle Linux 9 : kernel (ELSA-2024-12149)]	high
2/9/2024	[Oracle Linux 7 : runc (ELSA-2024-12148)]	high

Datum	Schwachstelle	Bewertung
2/9/2024	[Oracle Linux 7 : runc (ELSA-2024-17931)]	high
2/9/2024	[Mitsubishi MELSEC WS Ethernet Interface Modules Authentication Bypass (CVE-2023-6374)]	high
2/9/2024	[Rockwell ControlLogix and GuardLogix Controllers Denial of Service (CVE-2024-21916)]	high
2/11/2024	[Fedora 38 : runc (2024-9044c9eefa)]	high
2/11/2024	[Fedora 38 : webkitgtk (2024-ca3f071aea)]	high
2/11/2024	[Fedora 38 : wordpress (2024-df1cdcb0de)]	high
2/11/2024	[Fedora 38 : wireshark (2024-fdc7dfb959)]	high
2/11/2024	[IBM Java 8.0 < 8.0.8.20]	high
2/11/2024	[Fedora 39 : python-nikola (2024-262ad83644)]	high
2/11/2024	[Fedora 38 : chromium (2024-364516d49a)]	high
2/11/2024	[Fedora 38 : python-nikola (2024-1eb20f8ec3)]	high
2/10/2024	[Debian dsa-5619 : libgit2-1.1 - security update]	high
2/10/2024	[Fedora 39 : wordpress (2024-2b30739a76)]	high
2/10/2024	[Fedora 39 : wireshark (2024-b72131479b)]	high
2/10/2024	[AlmaLinux 9 : gimp (ALSA-2024:0675)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 09 Feb 2024

IBM i Access Client Solutions Remote Credential Theft

IBM i Access Client Solutions (ACS) versions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.4 suffer from a remote credential theft vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

Advanced Page Visit Counter 1.0 Cross Site Scripting

Advanced Page Visit Counter version 1.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

Online Nurse Hiring System 1.0 SQL Injection

Online Nurse Hiring System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

Rail Pass Management System 1.0 SQL Injection

Rail Pass Management System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

WordPress Augmented-Reality Remote Code Execution

WordPress Augmented-Reality plugin suffers from a remote code execution vulnerability. It is unclear which versions are affected.

- [Link](#)

—

” “Fri, 09 Feb 2024

WordPress Seotheme Shell Upload

WordPress Seotheme plugin suffers from a remote shell upload vulnerability. It is unclear which versions are affected.

- [Link](#)

—

” “Fri, 09 Feb 2024

Zyxel zysh Format String Proof Of Concept

Proof of concept format string exploit for Zyxel zysh. Multiple improper input validation flaws were identified in some CLI commands of Zyxel USG/ZyWALL series firmware versions 4.09 through 4.71, USG FLEX series firmware versions 4.50 through 5.21, ATP series firmware versions 4.32 through 5.21, VPN series firmware versions 4.30 through 5.21, NSG series firmware versions 1.00 through 1.33 Patch 4, NXC2500 firmware version 6.10(AAIG.3) and earlier versions, NAP203 firmware version 6.25(ABFA.7) and earlier versions, NWA50AX firmware version 6.25(ABYW.5) and earlier versions, WAC500 firmware version 6.30(ABVS.2) and earlier versions, and WAX510D firmware version 6.30(ABTF.2) and earlier versions, that could allow a local authenticated attacker to cause a buffer overflow or a system crash via a crafted payload.

- [Link](#)

—

” “Thu, 08 Feb 2024

KiTTY 0.76.1.13 Buffer Overflows

KiTTY versions 0.76.1.13 and below suffer from buffer overflows related to ANSI escape sequences. Two exploits are included as proof of concepts as well as a full documented breakdown of the issues.

- [Link](#)

—

” “Thu, 08 Feb 2024

KiTTY 0.76.1.13 Command Injection

KiTTY versions 0.76.1.13 and below suffer from a command injection vulnerability when getting a remote file through scp. It appears to leverage an ANSI escape sequence issue which is quite an interesting vector of attack.

- [Link](#)

—

” “Thu, 08 Feb 2024

MediaTek WLAN Driver Memory Corruption

The MediaTek WLAN driver has VFS read handlers that do not check buffer size leading to userland memory corruption.

- [Link](#)

—

” “Mon, 05 Feb 2024

Cacti pollers.php SQL Injection / Remote Code Execution

This Metasploit exploit module leverages sql injection and local file inclusion vulnerabilities in Cacti versions prior to 1.2.26 to achieve remote code execution. Authentication is needed and the account must have access to the vulnerable PHP script (pollers.php). This is granted by setting the Sites/Devices/Data permission in the General Administration section.

- [Link](#)

—

” “Mon, 05 Feb 2024

runc 1.1.11 File Descriptor Leak Privilege Escalation

runc versions 1.1.11 and below, as used by containerization technologies such as Docker engine and Kubernetes, are vulnerable to an arbitrary file write vulnerability. Due to a file descriptor leak it is possible to mount the host file system with the permissions of runc (typically root). Successfully tested on Ubuntu 22.04 with runc 1.1.7-0ubuntu1~22.04.1 using Docker build.

- [Link](#)

—

” “Mon, 05 Feb 2024

SISQUAL WFM 7.1.319.103 Host Header Injection

SISQUAL WFM version 7.1.319.103 suffers from a host header injection vulnerability.

- [Link](#)

—

” “Mon, 05 Feb 2024

Milesight UR5X / UR32L / UR32 / UR35 / UR41 Credential Leakage

Milesight IoT router versions UR5X, UR32L, UR32, UR35, and UR41 suffer from a credential leaking vulnerability due to unprotected system logs and weak password encryption.

- [Link](#)

—

” “Mon, 05 Feb 2024

Sumatra PDF 3.5.2 DLL Hijacking

Sumatra PDF version 3.5.2 suffers from a DLL hijacking vulnerability.

- [Link](#)

—

” “Mon, 05 Feb 2024

WordPress Simple URLs Cross Site Scripting

WordPress Simple URLs plugin versions prior to 115 suffer from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 05 Feb 2024

GYM MS 1.0 Cross Site Scripting

Gym Management System version 1.0 suffers from a persistent cross site scripting vulnerability. Original credit for this finding goes to Jyotsna Adhana in October of 2020 but uses a different vector of attack for this software version.

- [Link](#)

—

” “Mon, 05 Feb 2024

WhatsUp Gold 2022 22.1.0 Build 39 Cross Site Scripting

WhatsUp Gold 2022 version 22.1.0 Build 39 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 05 Feb 2024

MISP 2.4.171 Cross Site Scripting

MISP version 2.4.171 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 02 Feb 2024

Fortra GoAnywhere MFT Unauthenticated Remote Code Execution

This Metasploit module exploits a vulnerability in Fortra GoAnywhere MFT that allows an unauthenticated attacker to create a new administrator account. This can be leveraged to upload a JSP payload and achieve RCE. GoAnywhere MFT versions 6.x from 6.0.1, and 7.x before 7.4.1 are vulnerable.

- [Link](#)

—

” “Fri, 02 Feb 2024

Juniper SRX Firewall / EX Switch Remote Code Execution

This code serves as both a vulnerability detector and a proof of concept for CVE-2023-36845. It executes the phpinfo() function on the login page of the target device, allowing to inspect the PHP configuration. This script also has the option to save the phpinfo() output to a file for further analysis.

- [Link](#)

—

” “Fri, 02 Feb 2024

PCMan FTP Server 2.0 Buffer Overflow

PCMan FTP Server version 2.0 pwn remote buffer overflow exploit.

- [Link](#)

—

” “Fri, 02 Feb 2024

Proxmox VE 7.4-1 TOTP Brute Force

Proxmox VE versions 5.4 through 7.4-1 suffer from a TOTP brute forcing vulnerability.

- [Link](#)

—

” “Fri, 02 Feb 2024

TP-LINK TL-WR740N HTML Injection

TP-LINK TL-WR740N suffers from an html injection vulnerability.

- [Link](#)

—

” “Fri, 02 Feb 2024

GoAhead Web Server 2.5 HTML Injection

GoAhead Web Server version 2.5 suffers from an html injection vulnerability.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 09 Feb 2024

ZDI-24-123: X.Org Server DeviceFocusEvent Improper Validation of Array Index Local Privilege

Escalation Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-122: X.Org Server XIQueryPointer Improper Validation of Array Index Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-121: X.Org Server DeliverStateNotifyEvent Heap-based Buffer Overflow Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-120: X.Org Server XISendDeviceHierarchyEvent Heap-based Buffer Overflow Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-119: X.Org Server DisableDevice Heap-based Buffer Overflow Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-118: Centreon updateDirectory SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-117: Centreon updateGroups SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-116: Centreon updateLCARelation SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-115: Centreon updateContactServiceCommands SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-114: Centreon updateContactHostCommands SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-113: Centreon insertGraphTemplate SQL Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-112: Allegra downloadAttachmentGlobal Directory Traversal Information Disclosure Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-111: Allegra Hard-coded Credentials Authentication Bypass Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-110: Allegra downloadExportedChart Directory Traversal Authentication Bypass Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-109: Allegra uploadSimpleFile Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-108: Allegra saveInlineEdit Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-107: Allegra extarctZippedFile Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-106: Allegra renderFieldMatch Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-105: Allegra loadFieldMatch Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-104: Allegra saveFile Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-103: Allegra uploadFile Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-102: Allegra SiteConfigAction Improper Access Control Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-101: Allegra unzipFile Directory Traversal Remote Code Execution Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-100: Allegra serveMathJaxLibraries Directory Traversal Information Disclosure Vulnerability

- [Link](#)

—

” “Fri, 09 Feb 2024

ZDI-24-099: Allegra getFileContentAsString Directory Traversal Information Disclosure Vulnerability

- [Link](#)

—

” “Thu, 08 Feb 2024

ZDI-24-098: Schneider Electric Easergy Studio InitializeChannel Deserialization of Untrusted Data

Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Thu, 08 Feb 2024

ZDI-24-097: Wazuh Log Collector Integer Underflow Local Privilege Escalation Vulnerability

- [Link](#)

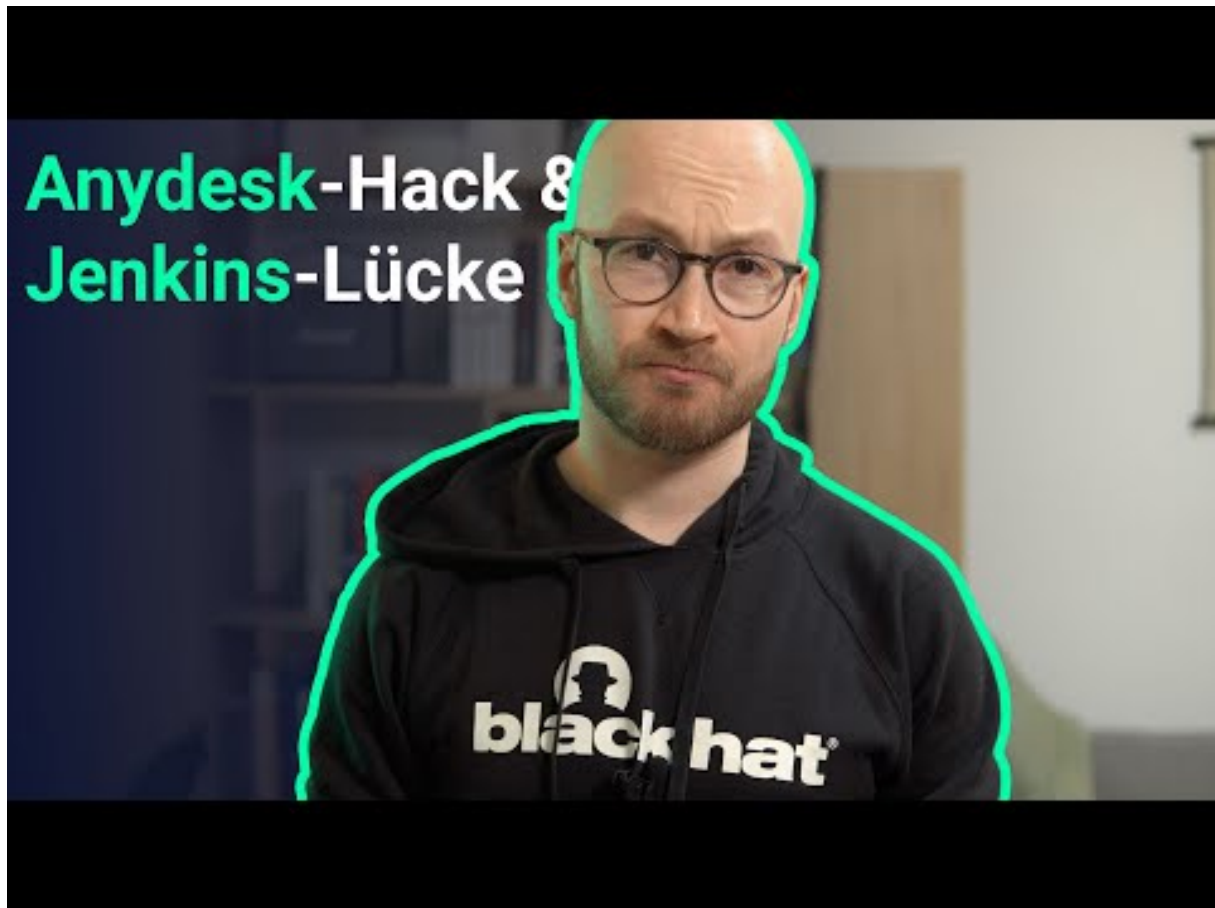
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 AnyDesk-Hack und Jenkins-Lücke



[Zum Youtube Video](#)

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-11	Centre hospitalier d'Armentières	[FRA]	Link
2024-02-07	Université de Central Missouri	[USA]	Link
2024-02-07	SouthState Bank	[USA]	Link
2024-02-07	Commune de Petersberg	[DEU]	Link
2024-02-07	Krankenhaus Lindenbrunn	[DEU]	Link
2024-02-06	Commune de Kalmar	[SWE]	Link
2024-02-06	Advania	[SWE]	Link
2024-02-04	Northern Light Health	[USA]	Link
2024-02-04	Middletown Area School District	[USA]	Link
2024-02-02	Germantown	[USA]	Link
2024-02-02	Universität de Reykjavík	[ISL]	Link
2024-02-02	Hôpital de la Trinité à Lippstadt, ainsi que les cliniques associées à Erwitte et Geseke.	[DEU]	Link
2024-02-02	Mairie de Korneuburg	[AUT]	Link
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	Link
2024-02-01	Ajuntament de Sant Antoni de Portmany	[ESP]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-12	[Kadac Australia]	medusa	Link
2024-02-11	[Amoskeag Network Consulting Group LLC]	medusa	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-11	[lacolline-skincare.com]	lockbit3	Link
2024-02-10	[Upper Merion Township]	qilin	Link
2024-02-10	[YKP LTDA]	ransomhub	Link
2024-02-10	[Village of Skokie]	hunters	Link
2024-02-10	[Lancaster County Sheriff's Office]	hunters	Link
2024-02-10	[Nastech]	hunters	Link
2024-02-10	[Benchmark Management Group]	hunters	Link
2024-02-10	[SOPEM Tunisie]	hunters	Link
2024-02-10	[Impact Energy Services]	hunters	Link
2024-02-10	[Groupe Goyette]	hunters	Link
2024-02-10	[Dalmahoy Hotel & Country Club]	hunters	Link
2024-02-10	[Carespring Health Care]	hunters	Link
2024-02-10	[Avianor Aircraft]	hunters	Link
2024-02-10	[mranet.org]	abyss	Link
2024-02-10	[aisg-online.com]	lockbit3	Link
2024-02-10	[maddockhenson]	alphv	Link
2024-02-10	[verdimed.es]	lockbit3	Link
2024-02-10	[Pacific American Fish Company Inc.]	incransom	Link
2024-02-09	[water.cc]	lockbit3	Link
2024-02-09	[CTSI]	bianlian	Link
2024-02-09	[J.P. Original]	bianlian	Link
2024-02-09	[TechNet Kronoberg AB]	bianlian	Link
2024-02-09	[Capozzi Adler, P.C.]	bianlian	Link
2024-02-09	[Drost Kivlahan McMahon & O'Connor LLC]	bianlian	Link
2024-02-09	[Grace Lutheran Foundation]	alphv	Link
2024-02-09	[ZGEO]	qilin	Link
2024-02-09	[alfiras.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-09	[wannago.cloud]	qilin	Link
2024-02-09	[grupomoraval.com]	lockbit3	Link
2024-02-09	[cdtmedicus.pl]	lockbit3	Link
2024-02-09	[soken-ce.co.jp]	lockbit3	Link
2024-02-09	[maximumresearch.com]	lockbit3	Link
2024-02-09	[indoramaventures.com]	lockbit3	Link
2024-02-09	[willislease.com]	blackbasta	Link
2024-02-09	[northseayachtsupport.nl]	lockbit3	Link
2024-02-09	[seymourct.org]	lockbit3	Link
2024-02-09	[bsaarchitects.com]	lockbit3	Link
2024-02-09	[moneyadvicetrust.org]	lockbit3	Link
2024-02-09	[posen.com]	abyss	Link
2024-02-09	[macqueeneq.com]	lockbit3	Link
2024-02-09	[parksite.com]	cactus	Link
2024-02-07	[galbusera.it]	lockbit3	Link
2024-02-08	[Ducont]	hunters	Link
2024-02-08	[perkinsmfg.com]	lockbit3	Link
2024-02-08	[originalfootwear.com]	lockbit3	Link
2024-02-08	[Jewish Home Lifecare]	alphv	Link
2024-02-08	[Distecna]	akira	Link
2024-02-07	[Western Municipal Construction]	blacksuit	Link
2024-02-07	[Southwest Binding & Laminating]	blacksuit	Link
2024-02-07	[TeraGo]	akira	Link
2024-02-07	[transaxle.com]	abyss	Link
2024-02-07	[Anderco PTE LTD]	8base	Link
2024-02-07	[Tetrosyl Group Limited]	8base	Link
2024-02-07	[Therme Laa Hotel and Silent Spa]	8base	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	Link
2024-02-07	[YRW Limited - Chartered Accountants]	8base	Link
2024-02-06	[axsbolivia.com]	lockbit3	Link
2024-02-06	[vimarequipment.com]	lockbit3	Link
2024-02-06	[deltron.com]	abyss	Link
2024-02-06	[B&B Electric Inc]	bianlian	Link
2024-02-06	[AVer Information]	akira	Link
2024-02-06	[Celeste]	akira	Link
2024-02-06	[ArpuPlus]	medusa	Link
2024-02-06	[gocco.com]	cactus	Link
2024-02-06	[spbglobal.com]	cactus	Link
2024-02-05	[Modern Kitchens]	play	Link
2024-02-05	[Greenwich Leisure]	play	Link
2024-02-05	[Ready Mixed Concrete]	play	Link
2024-02-05	[Northeastern Sheet Metal]	play	Link
2024-02-05	[Hannon Transport]	play	Link
2024-02-05	[McMillan Pazdan Smith]	play	Link
2024-02-05	[Mason Construction]	play	Link
2024-02-05	[Albert Bartlett]	play	Link
2024-02-05	[Perry-McCall Construction]	play	Link
2024-02-05	[Virgin Islands Lottery]	play	Link
2024-02-05	[Premier Facility Management]	play	Link
2024-02-05	[Douglas County Libraries]	play	Link
2024-02-05	[Leaders Staffing]	play	Link
2024-02-06	[asecos.com]	blackbasta	Link
2024-02-05	[GRUPO SCA Release of all data]]	knight	Link
2024-02-05	[themisbourne.co.uk]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	Link
2024-02-05	[hutchpaving.com]	lockbit3	Link
2024-02-05	[davis-french-associates.co.uk]	lockbit3	Link
2024-02-05	[Campaign for Tobacco-Free Kids]	blacksuit	Link
2024-02-05	[VCS Observation]	akira	Link
2024-02-05	[noe.wifi.at]	lockbit3	Link
2024-02-05	[ksa-architecture.com]	lockbit3	Link
2024-02-05	[GRTC Transit System]	bianlian	Link
2024-02-05	[semesco.com]	lockbit3	Link
2024-02-05	[ultraflexx.com]	lockbit3	Link
2024-02-05	[tgestiona.br]	lockbit3	Link
2024-02-05	[philogen.com]	lockbit3	Link
2024-02-05	[prima.com]	lockbit3	Link
2024-02-05	[logtainer.com]	lockbit3	Link
2024-02-05	[portline.pt]	lockbit3	Link
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	Link
2024-02-04	[cxm.com]	lockbit3	Link
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	Link
2024-02-04	[Commonwealth Sign]	qilin	Link
2024-02-04	[FEPCO Zona Franca SAS]	knight	Link
2024-02-03	[pbwtulsa.com]	lockbit3	Link
2024-02-02	[Digitel Venezuela]	medusa	Link
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	Link
2024-02-02	[manitou-group.com]	lockbit3	Link
2024-02-02	[AbelSantosyAsociados]	knight	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-02	[lexcaribbean.com]	lockbit3	Link
2024-02-02	[Law Office of Michael H Joseph]	bianlian	Link
2024-02-02	[Tandem]	bianlian	Link
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.