Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240209

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

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 bösartigen Akteuren die Ausweitung von Rechten.

- Link

—

VMware Aria-Schwachstellen ermöglichen Erhöhung der Zugriffsrechte

VMware hat Updates für VMware Aria Operations for Networks herausgegeben. Sie dichten Sicherheitslecks ab, die etwa die Ausweitung der Rechte ermöglichen.

- Link

—

Jetzt patchen! TeamCity-Schwachstelle ermöglicht Zugang ohne Authentifizierung

Ein Patch von JetBrains behebt eine kritische Schwachstelle in der On-Premises-Version des CI/CD-Servers.

- Link

—

Sicherheitsupdates: Dell schließt ältere Lücken in Backuplösungen wie Avamar

Schwachstellen in Komponenten von Drittanbietern gefährden die Sicherheit von Dell-Backup-Software. Sicherheitsupdates sind verfügbar.

- Link

—

Anydesk-Einbruch: Französisches BSI-Pendant vermutet Dezember als Einbruchsdatum

Die französische IT-Sicherheitsbehörde datiert die Anydesk-Kompromittierung auf Dezember 2023. Und empfiehlt die Deinstallation der Software.

- Link

—

Google Chrome: Update schließt mögliche Codeschmuggel-Lücken

Drei Sicherheitslücken schließt Google mit einem Chrome-Update. Angreifer können durch sie womöglich Schadcode 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-2023-6553	0.909010000	0.986320000	Link
CVE-2023-5360	0.967230000	0.995810000	Link
CVE-2023-4966	0.964760000	0.994830000	Link
CVE-2023-47246	0.911870000	0.986600000	Link
CVE-2023-46805	0.962740000	0.994200000	Link
CVE-2023-46747	0.971850000	0.997680000	Link
CVE-2023-46604	0.972850000	0.998270000	Link
CVE-2023-43177	0.932620000	0.988960000	Link
CVE-2023-42793	0.973130000	0.998460000	Link
CVE-2023-41265	0.902540000	0.985830000	Link
CVE-2023-39143	0.919450000	0.987390000	Link
CVE-2023-38205	0.932790000	0.988990000	Link
CVE-2023-38035	0.974110000	0.999140000	Link
CVE-2023-36845	0.971920000	0.997740000	Link
CVE-2023-3519	0.912410000	0.986670000	Link
CVE-2023-35082	0.962080000	0.994030000	Link
CVE-2023-35078	0.952060000	0.991810000	Link
CVE-2023-34960	0.931300000	0.988750000	Link
CVE-2023-34634	0.919000000	0.987340000	Link
CVE-2023-34362	0.960730000	0.993700000	Link
CVE-2023-3368	0.928930000	0.988480000	Link
CVE-2023-33246	0.973540000	0.998710000	Link
CVE-2023-32315	0.973860000	0.998930000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32235	0.902020000	0.985810000	Link
CVE-2023-30625	0.950540000	0.991470000	Link
CVE-2023-30013	0.936180000	0.989320000	Link
CVE-2023-29300	0.958470000	0.993170000	Link
CVE-2023-28771	0.923800000	0.987920000	Link
CVE-2023-28121	0.932010000	0.988810000	Link
CVE-2023-27524	0.972220000	0.997930000	Link
CVE-2023-27372	0.970420000	0.997020000	Link
CVE-2023-27350	0.972270000	0.997960000	Link
CVE-2023-26469	0.936750000	0.989420000	Link
CVE-2023-26360	0.956850000	0.992860000	Link
CVE-2023-26035	0.968710000	0.996380000	Link
CVE-2023-25717	0.964020000	0.994650000	Link
CVE-2023-25194	0.916080000	0.986980000	Link
CVE-2023-2479	0.964780000	0.994840000	Link
CVE-2023-24489	0.973640000	0.998770000	Link
CVE-2023-23752	0.949820000	0.991380000	Link
CVE-2023-23397	0.906590000	0.986090000	Link
CVE-2023-22527	0.974310000	0.999290000	Link
CVE-2023-22518	0.970760000	0.997160000	Link
CVE-2023-22515	0.962730000	0.994190000	Link
CVE-2023-21839	0.961800000	0.993960000	Link
CVE-2023-21823	0.940060000	0.989860000	Link
CVE-2023-21554	0.961220000	0.993800000	Link
CVE-2023-20887	0.965640000	0.995260000	Link
CVE-2023-20198	0.919220000	0.987360000	Link
CVE-2023-1671	0.965490000	0.995190000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-0669	0.968670000	0.996350000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

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

—

Thu, 08 Feb 2024

[NEU] [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

—

Thu, 08 Feb 2024

[NEU] [hoch] Cisco Expressway: Mehrere Schwachstellen

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

- Link

—

Thu, 08 Feb 2024

[NEU] [hoch] SonicWall SonicOS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in SonicWall SonicOS ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 08 Feb 2024

[NEU] [hoch] Graylog: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Graylog ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.

- Link

—

Thu, 08 Feb 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 08 Feb 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 08 Feb 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 08 Feb 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 08 Feb 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen und beliebigen Code zur Ausführung zu bringen.

- Link

—

Thu, 08 Feb 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel und Oracle Linux ausnutzen, um seine Privilegien zu erhöhen und Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 08 Feb 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 08 Feb 2024

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

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

- Link

—

Thu, 08 Feb 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 08 Feb 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Thu, 08 Feb 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff und einen nicht spezifizierten Angriff durchzuführen.
- Link

—

Thu, 08 Feb 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

—

Thu, 08 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

—

Thu, 08 Feb 2024

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/9/2024	[RHEL 8 : unbound (RHSA-2024:0749)]	critical
2/8/2024	[EulerOS 2.0 SP5 : kernel (EulerOS-SA-2024-1144)]	critical
2/8/2024	[EulerOS 2.0 SP5 : libplist (EulerOS-SA-2024-1147)]	critical
2/8/2024	[EulerOS 2.0 SP5 : python (EulerOS-SA-2024-1160)]	critical
2/8/2024	[EulerOS 2.0 SP9 : kernel (EulerOS-SA-2024-1196)]	critical

Datum	Schwachstelle	Bewertung
2/8/2024	[Mobotix S14 Camera Weak Password Requirements (CVE-2019-7674)]	critical
2/9/2024	[RHEL 8 : container-tools:rhel8 (RHSA-2024:0764)]	high
2/9/2024	[RHEL 8 : python-pillow (RHSA-2024:0754)]	high
2/9/2024	[RHEL 9 : gimp (RHSA-2024:0675)]	high
2/9/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libavif (SUSE-SU-2024:0423-1)]	high
2/9/2024	[SUSE SLES15 Security Update : kernel (Live Patch 21 for SLE 15 SP4) (SUSE-SU-2024:0429-1)]	high
2/9/2024	[SUSE SLES15 Security Update : kernel (Live Patch 20 for SLE 15 SP4) (SUSE-SU-2024:0428-1)]	high
2/9/2024	[Debian dsa-5618 : gir1.2-javascriptcoregtk-4.0 - security update]	high
2/8/2024	[EulerOS 2.0 SP5 : vim (EulerOS-SA-2024-1168)]	high
2/8/2024	[EulerOS 2.0 SP5 : gdb (EulerOS-SA-2024-1137)]	high
2/8/2024	[EulerOS 2.0 SP9 : libXpm (EulerOS-SA-2024-1180)]	high
2/8/2024	[EulerOS 2.0 SP9 : xorg-x11-server (EulerOS-SA-2024-1190)]	high
2/8/2024	[Fedora 38 : atril (2024-59a7d96d84)]	high
2/8/2024	[Fedora 39 : webkitgtk (2024-97faaca23d)]	high
2/8/2024	[Fedora 38 : gnutls (2024-c43a6cc3f8)]	high
2/8/2024	[Fedora 39 : chromium (2024-5745525066)]	high
2/8/2024	[Fedora 38 : python-aiohttp (2024-0ddda4c691)]	high
2/8/2024	[Mobotix S14 Camera Use of a Broken or Risky Cryptographic Algorithm (CVE-2019-7673)]	high
2/8/2024	[Mobotix S14 Camera Cross-Site Request Forgery (CSRF) (CVE-2019-12502)]	high
2/8/2024	[Mobotix S14 Camera Cleartext Transmission of Sensitive Information (CVE-2019-7675)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Fri, 02 Feb 2024

ComSndFTP Server 1.3.7 Beta Denial Of Service

ComSndFTP Server version 1.3.7 Beta remote denial of service exploit.

- Link

—

” “Fri, 02 Feb 2024

Ricoh Printer Directory / File Exposure

Ricoh printers suffer from directory and file exposure vulnerabilities.

- Link

—

” “Fri, 02 Feb 2024

Typora 1.7.4 Command Injection

Typora version 1.7.4 suffers from a command injection vulnerability.

- Link

—

” “Fri, 02 Feb 2024

Bank Locker Management System SQL Injection

Bank Locker Management System suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 02 Feb 2024

Grocy 4.0.2 Cross Site Request Forgery

Grocy versions 4.0.2 and below suffer from a cross site request forgery vulnerabilities.

- Link

—

” “Fri, 02 Feb 2024

WebCatalog 48.4 Arbitrary Protocol Execution / Code Execution

WebCatalog versions prior to 48.8 call the Electron shell.openExternal function without verifying that the URL is for an http or https resource. This vulnerability allows an attacker to potentially execute code through arbitrary protocols on the victims machine by having users sync pages with malicious URLs. The victim has to interact with the link, which can then enable an attacker to bypass security measures for malicious file delivery.

- Link

—

” “Fri, 02 Feb 2024

7 Sticky Notes 1.9 Command Injection

7 Sticky Notes version 1.9 suffers from a command injection vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 06 Feb 2024

ZDI-24-096: Oracle Product Lifecycle Management ExportServlet Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-095: Canon imageCLASS MF753Cdw Fax Job Heap-Based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-094: (Pwn2Own) Canon imageCLASS MF753Cdw CADM setResource Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-093: (Pwn2Own) Canon imageCLASS MF753Cdw SLP service-url Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-092: (Pwn2Own) Canon imageCLASS MF753Cdw rls-login Authorization Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-091: (Pwn2Own) Canon imageCLASS MF753Cdw Probe message Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-090: (Pwn2Own) Canon imageCLASS MF753Cdw rls-login Authorization Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-089: (Pwn2Own) Canon imageCLASS MF753Cdw CADM rmSetFileName Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-088: (Pwn2Own) Western Digital MyCloud PR4100 RESTSDK Uncontrolled Resource Consumption Denial-of-Service Vulnerability

- Link

—

” “Tue, 06 Feb 2024

ZDI-24-087: (Pwn2Own) Western Digital MyCloud PR4100 RESTSDK Server-Side Request Forgery Vulnerability

- Link

—

” “Mon, 05 Feb 2024

ZDI-24-086: TP-Link Omada ER605 Access Control Command Injection Remote Code Execution Vulnerability

- Link

—

” “Mon, 05 Feb 2024

ZDI-24-085: (Pwn2Own) TP-Link Omada ER605 DHCPv6 Client Options Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

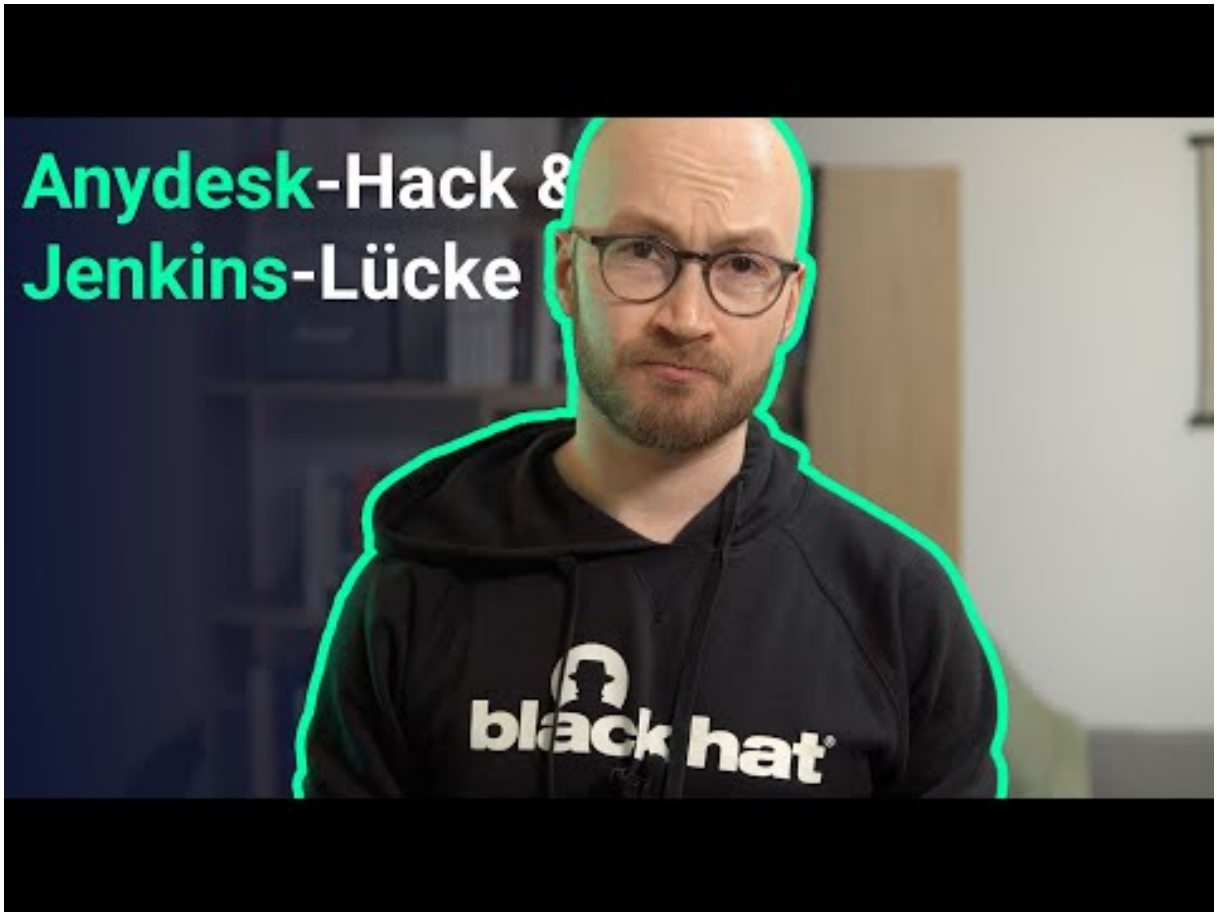
—

”

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
2024-02-02	Germantown	[USA]	Link
2024-02-02	Université de Reykjavík	[ISL]	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

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	Link
2024-02-07	[YRW Limited - Chartered Accountants]	8base	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2024-02-02	[lexcaribbean.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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.