Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240111

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

Zerodays bei Ivanti aktiv genutzt: Connect Secure und Policy Secure sinds nicht

Zwei Zero-Days in Ivanti-Produkten machen es “trivial für Angreifer”, Befehle auszuführen und sich im Firmennetz einzunisten. Ivanti hat bedingt gute Tipps.

- Link

—

Webkonferenzen: Zoom-Sicherheitslücken ermöglichen Rechteausweitung

Zoom verteilt aktualisierte Videokonferenz-Software. Sie schließt eine Sicherheitslücke, durch die Angreifer ihre Rechte ausweiten können.

- Link

—

Fortinet: Sicherheitsupdate gegen Rechteverwaltungsfehler in FortiOS und -Proxy

Fortinet warnt vor einem Fehler in der Rechteverwaltung von FortiOS und FortiProxy in HA Clustern. Bösartige Akteure können ihre Rechte ausweiten.

- Link

—

Patchday Adobe: Mehrere Schwachstellen in Substance 3D Stager geschlossen

Adobes Anwendung zum Erstellen von 3D-Szenen Substance 3D Stager ist angreifbar. Eine fehlerbereinigte Version steht zum Download bereit.

- Link

—

Patchday Microsoft: Kerberos-Authentifizierung unter Windows verwundbar

Es sind wichtige Sicherheitsupdates für Azure, Office, Windows und Co. erschienen. Attacken können bevorstehen. Ein Bitlocker-Patch macht Probleme.

- Link

—

Update für Google Chrome: Hochriskantes Sicherheitsleck abgedichtet

Google hat turnusgemäß den Webbrowser Chrome aktualisiert. Dabei haben die Entwickler eine als hohes Risiko eingestufte Sicherheitslücke gestopft.

- Link

—

Synology warnt vor Sicherheitslücke im DSM-Betriebssystem

Synology gibt eine Warnung vor einer Sicherheitslücke im DSM-Betriebssystem für NAS-Systeme heraus. Updates stehen länger bereit.

- Link

—

SAP-Patchday: Teils kritische Lücken in Geschäftssoftware

Der Januar-Patchday von SAP behandelt teils kritische Sicherheitslücken. Zu insgesamt zehn Schwachstellen gibt es Sicherheitsnotizen.

- Link

—

Jetzt patchen! Attacken auf Messaging-Plattform Apache RocketMQ

Angreifer scannen derzeit vermehrt nach verwundbaren RocketMQ-Servern. Sicherheitsupdates stehen bereit.

- Link

—

IBM warnt vor Sicherheitslücke in Db2

IBM warnt vor einer Sicherheitslücke in Db2. Angreifer können dadurch ihre Rechte in Windows-Systemen ausweiten. Updates stehen bereit.

- Link

—

3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-5360	0.967230000	0.995810000	Link
CVE-2023-4966	0.925220000	0.987920000	Link
CVE-2023-46747	0.965530000	0.995220000	Link
CVE-2023-46604	0.971470000	0.997580000	Link
CVE-2023-42793	0.972830000	0.998360000	Link
CVE-2023-38035	0.971630000	0.997650000	Link
CVE-2023-35078	0.948640000	0.991100000	Link
CVE-2023-34634	0.906880000	0.985860000	Link
CVE-2023-33246	0.971220000	0.997470000	Link
CVE-2023-32315	0.964530000	0.994800000	Link
CVE-2023-30625	0.937080000	0.989360000	Link
CVE-2023-30013	0.944370000	0.990360000	Link
CVE-2023-29300	0.933050000	0.988880000	Link
CVE-2023-28771	0.923800000	0.987750000	Link
CVE-2023-27524	0.962250000	0.994060000	Link
CVE-2023-27372	0.970430000	0.997020000	Link
CVE-2023-27350	0.972430000	0.998110000	Link
CVE-2023-26469	0.938510000	0.989510000	Link
CVE-2023-26360	0.942270000	0.989990000	Link
CVE-2023-26035	0.968020000	0.996100000	Link
CVE-2023-25717	0.954350000	0.992230000	Link
CVE-2023-25194	0.910840000	0.986250000	Link
CVE-2023-2479	0.958820000	0.993240000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.968700000	0.996360000	Link
CVE-2023-23752	0.961870000	0.993970000	Link
CVE-2023-22518	0.965250000	0.995070000	Link
CVE-2023-22515	0.955290000	0.992440000	Link
CVE-2023-21839	0.962040000	0.994030000	Link
CVE-2023-21823	0.940060000	0.989700000	Link
CVE-2023-21554	0.961220000	0.993770000	Link
CVE-2023-20887	0.961530000	0.993840000	Link
CVE-2023-1671	0.953130000	0.991960000	Link
CVE-2023-0669	0.968210000	0.996150000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 10 Jan 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

—

Wed, 10 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 10 Jan 2024

[NEU] [hoch] IBM Security Verify Access: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in IBM Security Verify Access ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder komplexe

Angriffe wie Cache Poisoning, Cross-Site-Scripting oder Session-Hijacking durchzuführen.
- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Wed, 10 Jan 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

—

Wed, 10 Jan 2024

[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung

Ein Angreifer in Funk-Reichweite kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 10 Jan 2024

[NEU] [hoch] Splunk Enterprise: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Splunk Enterprise ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder unbekannte Auswirkungen zu verursachen.
- Link

—

Wed, 10 Jan 2024

[NEU] [hoch] Fortinet FortiOS und Fortinet FortiProxy: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Fortinet FortiOS und Fortinet FortiProxy ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Wed, 10 Jan 2024

[NEU] [hoch] Lenovo Computer: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Lenovo Computer ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 10 Jan 2024

[NEU] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] libsndfile: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in libsndfile ausnutzen, um beliebigen Code auszuführen, einen ‘Denial of Service’-Zustand herbeizuführen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] binutils: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in binutils ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder sonstige Auswirkungen zu verursachen.

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 10 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 10 Jan 2024

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

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

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Wed, 10 Jan 2024

[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- Link

—

Wed, 10 Jan 2024

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen,

um beliebigen Programmcode auszuführen und einen Denial of Service Zustand zu verursachen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/10/2024	[RHEL 8 : fence-agents (RHSA-2024:0133)]	critical
1/10/2024	[RHEL 8 : frr (RHSA-2024:0130)]	critical
1/10/2024	[RHEL 8 : libarchive (RHSA-2024:0146)]	critical
1/10/2024	[Security Update for Microsoft .NET Core SDK (CVE-2024-0057)]	critical
1/10/2024	[Security Update for Microsoft .NET Core SDK (Jan 2024)]	critical
1/10/2024	[Security Updates for Microsoft .NET Framework (January 2024)]	critical
1/10/2024	[Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)]	critical
1/10/2024	[RHEL 9 : .NET 8.0 (RHSA-2024:0152)]	critical
1/10/2024	[RHEL 8 : .NET 6.0 (RHSA-2024:0158)]	critical
1/10/2024	[RHEL 8 : .NET 8.0 (RHSA-2024:0150)]	critical
1/10/2024	[RHEL 8 : .NET 7.0 (RHSA-2024:0157)]	critical
1/10/2024	[RHEL 9 : .NET 7.0 (RHSA-2024:0151)]	critical
1/10/2024	[RHEL 9 : .NET 6.0 (RHSA-2024:0156)]	critical
1/10/2024	[FreeBSD : chromium – security fix (ec8e4040-afcd-11ee-86bb-a8a1599412c6)]	critical
1/10/2024	[Fedora 39 : chromium (2024-01607ac0ae)]	critical
1/10/2024	[RHEL 8 : container-tools:4.0 (RHSA-2024:0121)]	high
1/10/2024	[RHEL 8 : pixman (RHSA-2024:0131)]	high

Datum	Schwachstelle	Bewertung
1/10/2024	[RHEL 8 : python3 (RHSA-2024:0114)]	high
1/10/2024	[RHEL 8 : kernel (RHSA-2024:0113)]	high
1/10/2024	[SAP NetWeaver AS ABAP HTTP Rapid Reset (Jan 2024)]	high
1/10/2024	[Fedora 38 : tigervnc / xorg-x11-server (2023-ec02e360af)]	high
1/10/2024	[Oracle Linux 8 : python-urllib3 (ELSA-2024-0116)]	high
1/10/2024	[Oracle Linux 8 : python3 (ELSA-2024-0114)]	high
1/10/2024	[Ubuntu 20.04 LTS : Linux kernel (IoT) vulnerabilities (USN-6548-5)]	high
1/10/2024	[Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-6549-5)]	high
1/10/2024	[Ubuntu 22.04 LTS : Linux kernel (OEM) vulnerability (USN-6576-1)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 10 Jan 2024

Android DeviceVersionFragment.java Privilege Escalation

Proof of concept exploit for a privilege escalation issue in Android. In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

- Link

—

” “Wed, 10 Jan 2024

PSOProxy 0.5 Denial Of Service

PSOProxy version 0.5 suffers from a denial of service vulnerability.

- Link

—

” “Wed, 10 Jan 2024

Backdoor.Win32 Carbanak (Anunak) MVID-2024-0667 Named Pipe NULL DACL

Backdoor.Win32 Carbanak (Anunak) malware creates 8 named pipes used for C2 and interprocess communications and grants RW access to the Everyone user group.

- Link

—

” “Tue, 09 Jan 2024

cpio 2.13 Privilege Escalation

cpio version 2.13 suffers from a privilege escalation vulnerability via setuid files in a cpio archive.

- Link

—

” “Tue, 09 Jan 2024

liveSite 2019.1 Remote Code Execution

liveSite version 2019.1 suffers from a remote code execution vulnerability.

- Link

—

” “Tue, 09 Jan 2024

Intrasrv Simple Web Server 1.0 Denial Of Service

Intrasrv Simple Web Server version 1.0 suffers from a denial of service vulnerability.

- Link

—

” “Tue, 09 Jan 2024

AdvantechWeb/SCADA 9.1.5U SQL Injection

AdvantechWeb/SCADA version 9.1.5U suffers from a post authentication remote SQL injection vulnerability.

- Link

—

” “Mon, 08 Jan 2024

iGalerie 3.0.22 Cross Site Scripting

iGalerie version 3.0.22 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Femitter FTP Server 1.03 Denial Of Service

Femitter FTP Server version 1.03 remote denial of service exploit.

- Link

—

” “Mon, 08 Jan 2024

PluXml Blog 5.8.9 Remote Code Execution

PluXml Blog version 5.8.9 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Linux 6.4 io_uring Use-After-Free

Linux versions 6.4 and above suffer from an io_uring page use-after-free vulnerability via buffer ring mmap.

- Link

—

” “Mon, 08 Jan 2024

io_uring __io_uaddr_map() Dangerous Multi-Page Handling

__io_uaddr_map() in io_uring suffers from dangerous handling of the multi-page region.

- Link

—

” “Mon, 08 Jan 2024

Form Tools 3.1.1 Cross Site Scripting

Form Tools version 3.1.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Gom Player 2.3.92.5362 Buffer Overflow

Gom Player version 2.3.92.5362 suffers from a buffer overflow vulnerability.

- Link

—

” “Mon, 08 Jan 2024

Gom Player 2.3.92.5362 DLL Hijacking

Gom Player version 2.3.92.5362 suffers from a dll hijacking vulnerability.

- Link

—

” “Mon, 08 Jan 2024

FreeSWITCH Denial Of Service

FreeSWITCH versions prior to 1.10.11 remote denial of service exploit that leverages a race condition in the hello handshake phase of the DTLS protocol.

- Link

—

” “Sun, 07 Jan 2024

File Sharing Wizard 1.5.0 Denial Of Service

File Sharing Wizard version 1.5.0 remote denial of service exploit.

- Link

—

” “Sat, 06 Jan 2024

httpdx 1.5.4 Denial Of Service

httpdx version 1.5.4 remote denial of service exploit.

- Link

—

” “Fri, 05 Jan 2024

Themebleed Windows 11 Themes Arbitrary Code Execution

When an unpatched Windows 11 host loads a theme file referencing an msstyles file, Windows loads the msstyles file, and if that file’s PACKME_VERSION is 999, it then attempts to load an accompanying dll file ending in _vrf.dll. Before loading that file, it verifies that the file is signed. It does this by opening the file for reading and verifying the signature before opening the file for execution. Because this action is performed in two discrete operations, it opens the procedure for a time of check to time of use vulnerability. By embedding a UNC file path to an SMB server we control, the SMB server can serve a legitimate, signed dll when queried for the read, but then serve a different file of the same name when the host intends to load/execute the dll.

- Link

—

” “Fri, 05 Jan 2024

Easy Chat Server 3.1 Denial Of Service

Easy Chat Server version 3.1 suffers from a denial of service vulnerability.

- Link

—

” “Thu, 04 Jan 2024

Easy File Sharing FTP Server 2.0 Denial Of Service

Easy File Sharing FTP Server version 2.0 suffers from a denial of service vulnerability.

- Link

—

” “Wed, 03 Jan 2024

minaliC 2.0.0 Denial Of Service

minaliC version 2.0.0 suffers from a denial of service vulnerability.

- Link

—

” “Wed, 03 Jan 2024

Microsoft Windows Kernel Information Disclosure

Any unprivileged, local user in Microsoft Windows can disclose whether a specific file, directory or registry key exists in the system or not, even if they do not have the open right to it or enumerate right to its parent.

- Link

—

” “Wed, 03 Jan 2024

Chrome BindTextSuggestionHostForFrame Type Confusion

Chrome suffers from a type confusion vulnerability in BindTextSuggestionHostForFrame.

- Link

—

” “Wed, 03 Jan 2024

WebCalendar 1.3.0 Cross Site Scripting

WebCalendar version 1.3.0 suffers from reflective and persistent cross site scripting vulnerabilities.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 10 Jan 2024

ZDI-24-032: Foxit PDF Reader Doc Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-031: Microsoft Windows cldflt Integer Overflow Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-030: Microsoft Office Word FBX File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-029: Trend Micro Apex One Exposed Dangerous Function Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-028: Trend Micro Apex One Security Agent Updater Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-027: Trend Micro Apex One Anti-Spyware Engine Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-026: Trend Micro Apex One Virus Scan Engine Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-025: Trend Micro Apex One Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-024: Trend Micro Apex Central widget WFProxy Local File Inclusion Remote Code Execution Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-023: Trend Micro Apex Central Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-022: Trend Micro Apex Central Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

” “Wed, 10 Jan 2024

ZDI-24-021: Trend Micro Apex Central Cross-Site Scripting Remote Code Execution Vulnerability

- Link

—

” “Tue, 09 Jan 2024

ZDI-24-020: Linux Kernel GSM Multiplexing Race Condition Local Privilege Escalation Vulnerability

- Link

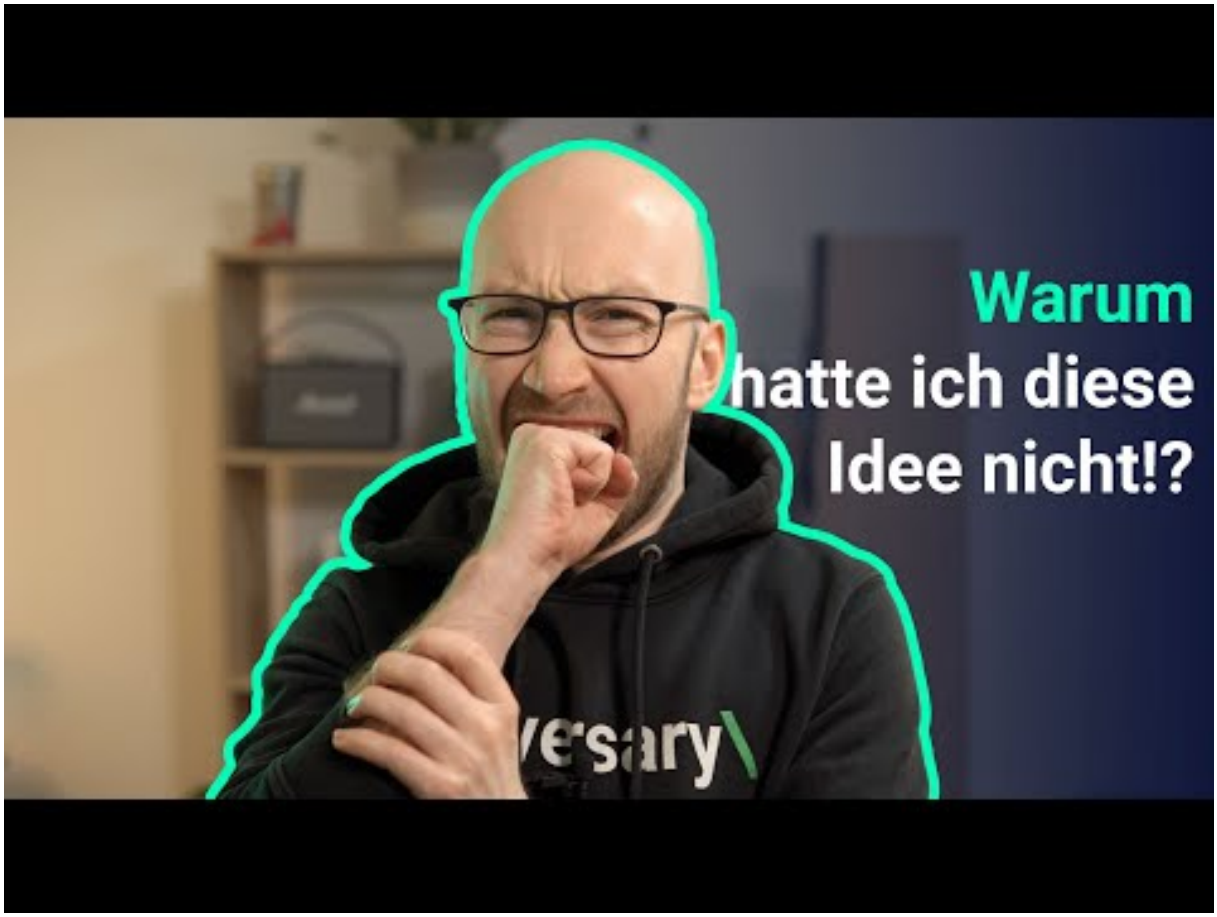
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Diese Idee hätte ich WIRKLICH gerne selbst gehabt (über 100k Bug Bounty)



Zum Youtube Video

6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-06	loanDepot	[USA]	Link
2024-01-05	Toronto Zoo	[CAN]	Link
2024-01-05	ODAV AG	[DEU]	Link
2024-01-04	City of Beckley	[USA]	Link
2024-01-04	Tigo Business	[PRY]	Link
2024-01-01	Commune de Saint-Philippe	[FRA]	Link

7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-10	[molnar&partner]	qilin	Link
2024-01-10	[hartalega.com.my]	lockbit3	Link
2024-01-10	[agnesb.eu]	lockbit3	Link
2024-01-10	[twt.co.za]	lockbit3	Link
2024-01-10	[tiautoinvestments.co.za]	lockbit3	Link
2024-01-10	[Group Bogart]	alphv	Link
2024-01-09	[Delco Automation]	blacksuit	Link
2024-01-09	[Viridi]	akira	Link
2024-01-09	[Ito Pallpack Gruppen]	akira	Link
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	Link
2024-01-09	[Precision Tune Auto Care]	8base	Link
2024-01-08	[Erbilbil Bilgisayar]	alphv	Link
2024-01-08	[HALLEONARD]	qilin	Link
2024-01-08	[Van Buren Public Schools]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-08	[Heller Industries]	akira	Link
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	Link
2024-01-08	[mciwv.com]	lockbit3	Link
2024-01-08	[morganpilate.com]	lockbit3	Link
2024-01-07	[capitalhealth.org]	lockbit3	Link
2024-01-07	[Flash-Motors Last Warning]	raznatovic	Link
2024-01-07	[Agro Baggio LTDA]	knight	Link
2024-01-06	[Maas911.com]	cloak	Link
2024-01-06	[GRUPO SCA]	knight	Link
2024-01-06	[Televerde]	play	Link
2024-01-06	[The Lutheran World Federation]	rhysida	Link
2024-01-05	[Proax Technologies LTD]	bianlian	Link
2024-01-05	[Somerset Logistics]	bianlian	Link
2024-01-05	[ips-securex.com]	lockbit3	Link
2024-01-04	[Project M.O.R.E.]	hunters	Link
2024-01-04	[Thermosash Commercial Ltd]	hunters	Link
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	Link
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	Link
2024-01-03	[Kershaw County School District]	blacksuit	Link
2024-01-03	[Bradford Health]	hunters	Link
2024-01-02	[groupe-idea.com]	lockbit3	Link
2024-01-02	[SAED International]	alphv	Link
2024-01-02	[graebener-group.com]	blackbasta	Link
2024-01-02	[leonardsexpress.com]	blackbasta	Link
2024-01-02	[nals.com]	blackbasta	Link
2024-01-02	[MPM Medical Supply]	ciphbit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-01-01	[DELPHINUS.COM]	clop	Link
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	Link

8 Quellen

8.1 Quellenverzeichnis

1) Cyberwatch - https://github.com/Casualtek/Cyberwatch
2) Ransomware.live - https://data.ransomware.live
3) Heise Security Alerts! - https://www.heise.de/security/alerts/
4) First EPSS - https://www.first.org/epss/
5) BSI WID - https://wid.cert-bund.de/
6) Tenable Plugins - https://www.tenable.com/plugins/
7) Exploit - packetstormsecurity.com
8) 0-Day - https://www.zerodayinitiative.com/rss/published/
9) Die Hacks der Woche - https://martinhaunschmid.com/videos

9 Impressum

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.