Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240408

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

Dell-Server: BIOS-Lücke als Einfallstor für Angreifer

Ein wichtiges Sicherheitsupdate schließt eine Schwachstelle im BIOS von Servern des Computerherstellers Dell.

- Link

—

Lexmark: Hochriskante Lücken erlauben Codeschmuggel auf Drucker

Lexmark warnt vor Sicherheitslücken in diversen Drucker-Firmwares. Angreifer können Schadcode einschleusen. Updates sind verfügbar.

- Link

—

Sicherheitslücken: DoS-Attacken auf IBM-Datenbank Db2 möglich

Angreifer können an mehreren Lücken in IBM App Connect Enterprise, Db2 und Rational Build Forge ansetzen.

- Link

—

Sicherheitsupdates für Ivanti: Schadcode kann durch VPN-Verbindungen schlüpfen

Es sind wichtige Sicherheitspatches für Ivanti Connect Secure und Policy Secure Gateways erschienen.

- Link

—

Cisco dichtet Schwachstellen in mehreren Produkten ab

Cisco hat zwölf Sicherheitsmitteilungen veröffentlicht. Die zugehörigen Updates dichten zahlreiche Sicherheitslücken ab.

- Link

—

Patchday Android: Angreifer können sich höhere Rechte verschaffen

Neben Google haben auch Samsung und weitere Hersteller wichtige Sicherheitsupdates für Androidgeräte veröffentlicht.

- Link

—

Kritische Sicherheitslücke in Wordpress-Plug-in Layerslider

IT-Forscher haben eine kritische Lücke im Wordpress-Plug-in Layerslider entdeckt. Es ist auf mehr als einer Million Seiten installiert.

- Link

—

Codeschmuggellücke in VMware SD-WAN Edge und Orchestrator

Drei Sicherheitslücken in VMwares SD-WAN Edge und Orchestrator ermöglichen Angreifern unter anderem, Schadcode einzuschleusen.

- Link

—

Google Chrome: Entwickler dichten drei Lücken ab, arbeiten an Cookie-Schutz

Im Webbrowser Chrome wurden drei Sicherheitslücken entdeckt. Google arbeitet zudem an Mechanismen gegen Cookie-Diebstahl.

- Link

—

Synology Surveillance Station: Mehrere Lücken gefährden Sicherheit

In der Software Surveillance Station von Synology klaffen Sicherheitslecks, die Angreifern etwa Codeschmuggel erlauben. Updates stopfen sie.

- 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	0.987430000	Link
CVE-2023-6553	0.916210000	0.988470000	Link
CVE-2023-5360	0.967230000	0.996410000	Link
CVE-2023-4966	0.964860000	0.995670000	Link
CVE-2023-47246	0.940270000	0.991110000	Link
CVE-2023-46805	0.964290000	0.995540000	Link
CVE-2023-46747	0.971350000	0.997820000	Link
CVE-2023-46604	0.973060000	0.998600000	Link
CVE-2023-43177	0.927670000	0.989770000	Link
CVE-2023-42793	0.970710000	0.997530000	Link
CVE-2023-39143	0.942940000	0.991470000	Link
CVE-2023-38646	0.928720000	0.989840000	Link
CVE-2023-38203	0.958450000	0.994080000	Link
CVE-2023-38035	0.972180000	0.998170000	Link
CVE-2023-36845	0.966640000	0.996230000	Link
CVE-2023-35813	0.905250000	0.987650000	Link
CVE-2023-3519	0.925380000	0.989490000	Link
CVE-2023-35082	0.950590000	0.992740000	Link
CVE-2023-35078	0.962310000	0.994950000	Link
CVE-2023-34993	0.944980000	0.991880000	Link
CVE-2023-34960	0.935410000	0.990570000	Link
CVE-2023-34634	0.925600000	0.989510000	Link
CVE-2023-34362	0.962490000	0.994990000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.907130000	0.987820000	Link
CVE-2023-3368	0.906550000	0.987740000	Link
CVE-2023-33246	0.973150000	0.998660000	Link
CVE-2023-32315	0.973840000	0.999060000	Link
CVE-2023-32235	0.911650000	0.988140000	Link
CVE-2023-30625	0.948330000	0.992410000	Link
CVE-2023-30013	0.956380000	0.993740000	Link
CVE-2023-29300	0.963460000	0.995270000	Link
CVE-2023-29298	0.926460000	0.989600000	Link
CVE-2023-28771	0.921620000	0.988990000	Link
CVE-2023-28432	0.943220000	0.991540000	Link
CVE-2023-28121	0.943690000	0.991610000	Link
CVE-2023-27524	0.972950000	0.998550000	Link
CVE-2023-27372	0.973490000	0.998880000	Link
CVE-2023-27350	0.972040000	0.998100000	Link
CVE-2023-26469	0.938630000	0.990930000	Link
CVE-2023-26360	0.963570000	0.995300000	Link
CVE-2023-26035	0.969280000	0.997030000	Link
CVE-2023-25717	0.957880000	0.993980000	Link
CVE-2023-25194	0.969270000	0.997030000	Link
CVE-2023-2479	0.963600000	0.995310000	Link
CVE-2023-24489	0.973810000	0.999040000	Link
CVE-2023-23752	0.952140000	0.992980000	Link
CVE-2023-23397	0.923530000	0.989200000	Link
CVE-2023-23333	0.963260000	0.995200000	Link
CVE-2023-22527	0.965680000	0.996000000	Link
CVE-2023-22518	0.969490000	0.997100000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22515	0.971880000	0.998030000	Link
CVE-2023-21839	0.958450000	0.994080000	Link
CVE-2023-21554	0.959700000	0.994340000	Link
CVE-2023-20887	0.964080000	0.995460000	Link
CVE-2023-1671	0.965610000	0.995990000	Link
CVE-2023-0669	0.969030000	0.996950000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 05 Apr 2024

[NEU] [hoch] Apache CloudStack: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache CloudStack ausnutzen, um die Authentifizierung zu umgehen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern und so die Kontrolle über das System zu übernehmen.

- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen Manipulation von Daten

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um Daten zu manipulieren.

- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] ESRI Portal for ArcGIS: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in ESRI ArcGIS ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Fri, 05 Apr 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

—

Fri, 05 Apr 2024

[NEU] [hoch] Broadcom Fabric OS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Broadcom Fabric OS ausnutzen, um beliebigen Code auszuführen und um falsche Informationen darzustellen.

- Link

—

Fri, 05 Apr 2024

[NEU] [hoch] Dell ECS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Dell ECS ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode mit Administratorrechten auszuführen, Informationen offenzulegen, Dateien zu manipulieren, einen Cross-Site-Scripting-Angriff durchzuführen, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] WordPress: Mehrere Schwachstellen

Ein entfernter authentifizierter Angreifer kann eine Schwachstelle in WordPress ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder beliebigen Code auszuführen.

- Link

—

Fri, 05 Apr 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, 05 Apr 2024

[UPDATE] [hoch] Squid: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Fri, 05 Apr 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

—

Fri, 05 Apr 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

—

Fri, 05 Apr 2024

[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen

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

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] Squid: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Fri, 05 Apr 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Fri, 05 Apr 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 potenziell Code auszuführen und um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 04 Apr 2024

[NEU] [hoch] Ivanti Connect Secure und Policy Secure: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure und Ivanti Policy Secure ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- Link

—

Thu, 04 Apr 2024

[NEU] [hoch] Lexmark Multifunction Printer: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer kann mehrere Schwachstellen in Lexmark Multifunction Printer ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 04 Apr 2024

[NEU] [hoch] IBM Security Verify Access: Schwachstelle ermöglicht Denial of Service oder Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM Security Verify Access ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- Link

—

Thu, 04 Apr 2024

[UPDATE] [hoch] expat: Schwachstelle ermöglicht Codeausführung

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

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/5/2024	[Fedora 39 : chromium (2024-39b249a59c)]	critical
4/4/2024	[Debian dsa-5654 : chromium - security update]	critical
4/4/2024	[Fedora 38 : chromium (2024-5e32ce95a3)]	critical
4/6/2024	[Debian dla-3779 : libtomcat9-embed-java - security update]	high
4/6/2024	[FreeBSD : Apache httpd – multiple vulnerabilities (8e6f684b-f333-11ee-a573-84a93843eb75)]	high
4/6/2024	[Debian dla-3780 : jetty9 - security update]	high
4/5/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : X.Org X Server vulnerabilities (USN-6721-1)]	high
4/5/2024	[OracleVM 3.4 : kernel-uek (OVMSA-2024-0004)]	high
4/5/2024	[Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3, 2024 Security Releases).]	high
4/5/2024	[Dell Client BIOS Privilege Escalation (DSA-2024-035)]	high
4/5/2024	[Slackware Linux 15.0 / current tigervnc Multiple Vulnerabilities (SSA:2024-096-01)]	high
4/5/2024	[Rocky Linux 9 : ruby:3.1 (RLSA-2024:1576)]	high
4/5/2024	[Rocky Linux 8 : kernel-rt (RLSA-2024:1614)]	high
4/5/2024	[Rocky Linux 8 : less (RLSA-2024:1610)]	high
4/5/2024	[Rocky Linux 8 : grafana (RLSA-2024:1646)]	high
4/5/2024	[Rocky Linux 8 : kernel (RLSA-2024:1607)]	high
4/5/2024	[Rocky Linux 8 : grafana-pcp (RLSA-2024:1644)]	high
4/5/2024	[Rocky Linux 8 : expat (RLSA-2024:1615)]	high
4/4/2024	[Slackware Linux 15.0 / current xorg-server Multiple Vulnerabilities (SSA:2024-094-01)]	high
4/4/2024	[Cisco Access Points Managed from WLC DoS (cisco-sa-ap-dos-h9TGGX6W)]	high

Datum	Schwachstelle	Bewertung
4/4/2024	[Cisco Access Points Managed from Catalyst DoS (cisco-sa-ap-dos-h9TGGX6W)]	high
4/4/2024	[CBL Mariner 2.0 Security Update: openwsman (CVE-2019-3816)]	high
4/4/2024	[CBL Mariner 2.0 Security Update: openwsman (CVE-2019-3833)]	high
4/4/2024	[Apache 2.4.x < 2.4.59 Multiple Vulnerabilities]	high
4/4/2024	[FreeBSD : xorg server – Multiple vulnerabilities (57561cfc-f24b-11ee-9730-001fc69cd6dc)]	high
4/4/2024	[Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2024-21894)]	high
4/4/2024	[Ivanti Policy Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2024-21894)]	high
4/4/2024	[RHEL 9 : nodejs (RHSA-2024:1678)]	high
4/4/2024	[Slackware Linux 15.0 / current httpd Multiple Vulnerabilities (SSA:2024-095-01)]	high
4/4/2024	[IBM WebSphere Application Server 8.5.5.3 < 8.5.5.26 / 9.x < 9.0.5.20 / Liberty 21.0.0.3 < 24.0.0.4 DoS (7145942)]	high
4/3/2024	[Westermo DR-250, DR-260 and MR-260 Unrestricted Upload of File with Dangerous Type (CVE-2018-19612)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 05 Apr 2024

Visual Planning 8 Arbitrary File Read

Authenticated attackers can exploit a weakness in the XML parser functionality of the Visual Planning application in order to obtain read access to arbitrary files on the application server. Depending on configured access permissions, this vulnerability could be used by an attacker to exfiltrate secrets stored on the local file system. All versions prior to Visual Planning 8 (Build 240207) are affected.

- Link

—

” “Fri, 05 Apr 2024

Visual Planning 8 Authentication Bypass

Unauthenticated attackers can exploit a weakness in the password reset functionality of the Visual Planning application in order to obtain access to arbitrary user accounts including administrators. In case administrative (in the context of Visual Planning) accounts are compromised, attackers can install malicious modules into the application to take over the application server hosting the Visual Planning application. All versions prior to Visual Planning 8 (Build 240207) are affected.

- Link

—

” “Fri, 05 Apr 2024

Visual Planning REST API 2.0 Authentication Bypass

A wildcard injection inside a prepared SQL statement was found in an undocumented Visual Planning 8 REST API route. The combination of fuzzy matching (via LIKE operator) and user-controlled input allows exfiltrating the REST API key based on distinguishable server responses. If exploited, attackers are able to gain administrative access to the REST API version 2.0.

- Link

—

” “Fri, 05 Apr 2024

Feng Office 3.10.8.21 Cross Site Scripting

Feng Office version 3.10.8.21 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 print/render/racer.inc SQL Injection

DerbyNet 9.0 suffers from a remote SQL injection vulnerability in print/render/racer.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 print/render/award.inc SQL Injection

DerbyNet 9.0 suffers from a remote SQL injection vulnerability in print/render/award.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 ajax/query.slide.next.inc SQL Injection

DerbyNet 9.0 suffers from a remote SQL injection vulnerability in ajax/query.slide.next.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 playlist.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in playlist.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 racer-results.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in racer-results.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 inc/kisosks.inc Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in inc/kiosks.inc.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 photo-thumbs.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in photo-thumbs.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 checkin.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in checkin.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 photo.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in photo.php.

- Link

—

” “Fri, 05 Apr 2024

DerbyNet 9.0 render-document.php Cross Site Scripting

DerbyNet version 9.0 suffers from a cross site scripting vulnerability in render-document.php.

- Link

—

” “Fri, 05 Apr 2024

Seo Panel 4.7.0 Cross Site Scripting

Seo Panel version 4.7.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 05 Apr 2024

Human Resource Management System 2024 1.0 SQL Injection

Human Resource Management System 2024 version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 05 Apr 2024

Jasmin Ransomware 1.1 Arbitrary File Read

Jasmin Ransomware version 1.1 suffers from an arbitrary file read vulnerability.

- Link

—

” “Fri, 05 Apr 2024

Gibbon School Platform 26.0.00 Remote Code Execution

A remote code execution vulnerability in Gibbon online school platform version 26.0.00 and lower allows remote authenticated users to conduct PHP deserialization attacks via columnOrder in a POST request to the endpoint /modules/System%20Admin/import_run.php&type=externalAssessment&step=4. As it allows remote code execution, adversaries could exploit this flaw to execute arbitrary commands, potentially resulting in complete system compromise, data exfiltration, or unauthorized access to sensitive information.

- Link

—

” “Fri, 05 Apr 2024

Linux 6.5 Kernel Pointer Leak

Linux versions starting with 6.5 suffer from a read-after-type-change of folio in cachestat() that leads to a kernel pointer leak.

- Link

—

” “Thu, 04 Apr 2024

Positron Broadcast Signal Processor TRA7005 1.20 Authentication Bypass

The Positron Broadcast Digital Signal Processor TRA7005 version 1.20 suffers from an authentication bypass through a direct and unauthorized access to the password management functionality. The vulnerability allows attackers to bypass Digest authentication by manipulating the password endpoint _Passwd.html and its payload data to set a user’s password to arbitrary value or remove it entirely. This grants unauthorized access to protected areas (/user, /operator, /admin) of the application without requiring valid credentials, compromising the device’s system security.

- Link

—

” “Thu, 04 Apr 2024

User Registration And Login And User Management System 3.2 SQL Injection

User Registration and Login and User Management System version 3.2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 04 Apr 2024

WordPress Membership For WooCommerce Shell Upload

WordPress Membership for WooCommerce plugin versions prior to 2.1.7 suffer from a remote shell upload vulnerability.

- Link

—

” “Wed, 03 Apr 2024

Google Pixel MFC H264 Processing Memory Corruption

There is a memory corruption issue in the MFC media processing core on the Pixel 7. It occurs when decoding a malformed H264 stream in Chrome, likely to due to an out of bounds quantization parameter. A write to plane 0 that occurs during macroblock decoding extends past the allocated bounds of the plane, and can overwrite the motion vector (MV) buffer or cause a crash if the adjacent address is unmapped. Both of these allocations are DMA buffers and it is unclear whether this condition is exploitable.

- Link

—

” “Wed, 03 Apr 2024

SUPERAntiSpyware Professional X 10.0.1264 DLL Hijacking / Privilege Escalation

SUPERAntiSpyware Professional X versions 10.0.1264 and below suffer from a privilege escalation vulnerability via dll hijacking.

- Link

—

” “Wed, 03 Apr 2024

WordPress Alemha Watermarker 1.3.1 Cross Site Scripting

WordPress Alemha Watermarker plugin version 1.3.1 suffers from a persistent cross site scripting vulnerability.

- Link

—

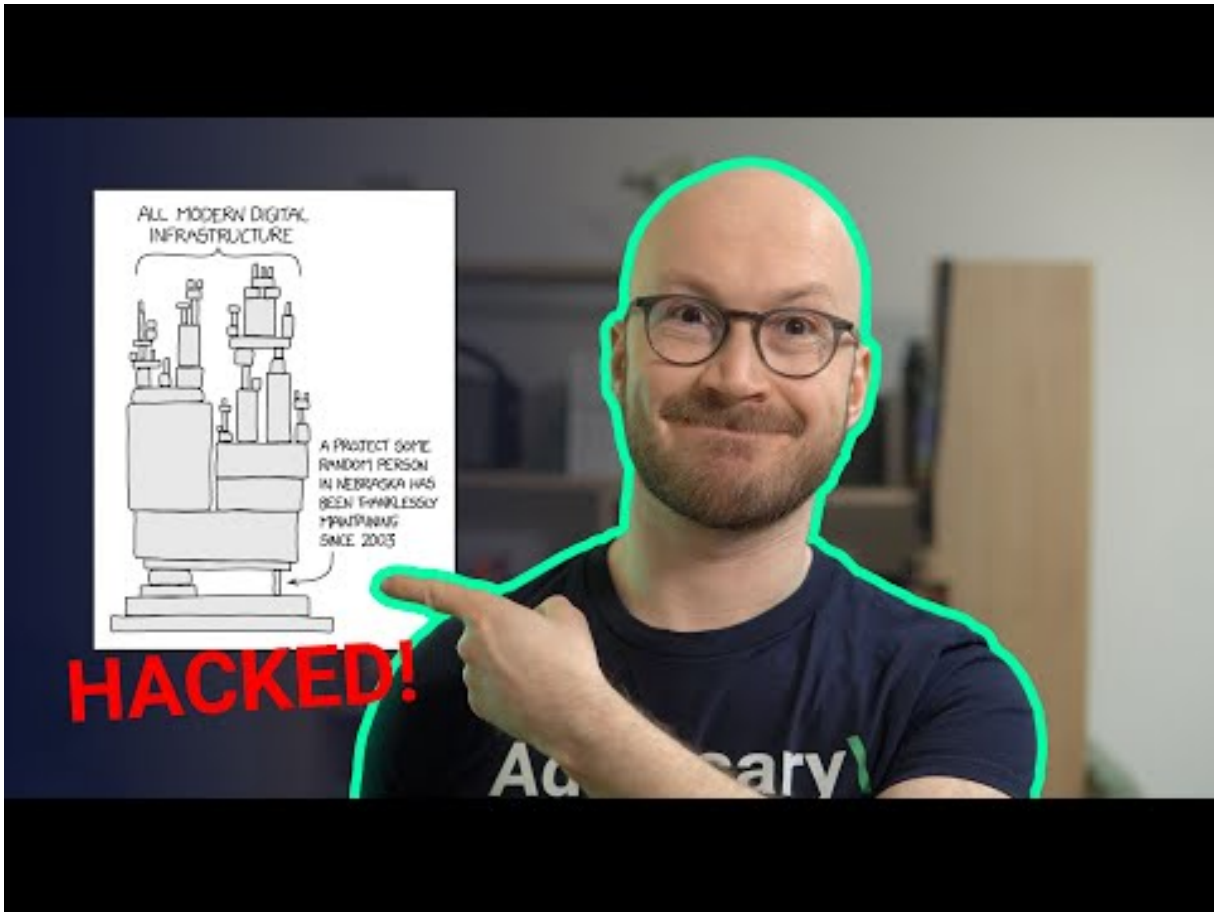
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Oh wow, this was *very* close: xz-utils was backdoored



Zum Youtube Video

6 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information
2024-04-04	Communauté de communes du bassin mussipontain	[FRA]	Link
2024-04-02	Comté de Jackson	[USA]	Link
2024-04-02	Prepay Technologies	[ESP]	Link

7 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-08	[Change HealthCare - OPTUM Group - United HealthCare Group]	ransomhub	Link
2024-04-07	[PalauGov]	dragonforce	Link
2024-04-07	[Ellsworth Cooperative Creamery]	blacksuit	Link
2024-04-07	[SERVICES INFORMATIQUES POUR PROFESSIONNELS(SIP)]	blacksuit	Link
2024-04-07	[Malaysian Industrial Development Finance]	rhysida	Link
2024-04-07	[easchangesystems]	qilin	Link
2024-04-06	[Carrozzeria Aretusa srl]	ransomhub	Link
2024-04-06	[HCI Systems, Inc.]	ransomhub	Link
2024-04-06	[Madero]	qilin	Link
2024-04-06	[Chambers Construction]	bianlian	Link
2024-04-06	[On Q Financial, LLC]	bianlian	Link
2024-04-06	[Better Accounting Solutions]	ransomhub	Link
2024-04-06	[TermoPlastic S.R.L]	ciphbit	Link
2024-04-05	[truehomes.com]	lockbit3	Link
2024-04-04	[Good Morning]	donutleaks	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-05	[casio india]	stormous	Link
2024-04-05	[emalon.co.il]	malekteam	Link
2024-04-05	[Aussizz Group]	dragonforce	Link
2024-04-05	[Doctorim]	malekteam	Link
2024-04-05	[Agencia Host]	ransomhub	Link
2024-04-05	[Commerce Dental Group]	ciphbit	Link
2024-04-04	[Sit]	play	Link
2024-04-04	[Guy’s Floor Service]	play	Link
2024-04-04	[Everbrite]	play	Link
2024-04-03	[Orientrose Contracts]	medusa	Link
2024-04-03	[Sutton Dental Arts]	medusa	Link
2024-04-04	[Inspection Services]	akira	Link
2024-04-04	[Radiant Canada]	akira	Link
2024-04-04	[Constelacion Savings and Credit Society]	ransomhub	Link
2024-04-04	[Remitano - Cryptocurrency Exchange]	incransom	Link
2024-04-04	[mcalvain.com]	cactus	Link
2024-04-03	[Precision Pulley & Idler]	blacksuit	Link
2024-04-03	[Wacks Law Group]	qilin	Link
2024-04-03	[BeneCare Dental Insurance]	hunters	Link
2024-04-03	[Interface]	hunters	Link
2024-04-03	[DataBank]	hunters	Link
2024-04-03	[Beaver Run Resort]	hunters	Link
2024-04-03	[Benetton Group]	hunters	Link
2024-04-03	[Citi Trends]	hunters	Link
2024-04-03	[Intersport]	hunters	Link
2024-04-03	[West Idaho Orthopedics]	incransom	Link
2024-04-03	[Norman Urology Associates]	incransom	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-03	[Phillip Townsend Associates]	blacksuit	Link
2024-04-02	[San Pasqual Band of Mission Indians]	medusa	Link
2024-04-02	[East Baton Rouge Sheriff’s Office]	medusa	Link
2024-04-03	[Leicester City Council]	incransom	Link
2024-04-03	[Ringhoffer Verzahnungstechnik GmbH and Co. KG]	8base	Link
2024-04-03	[Samhwa Paint Ind. Ltd]	8base	Link
2024-04-03	[Tamura Corporation]	8base	Link
2024-04-03	[Apex Business Advisory]	8base	Link
2024-04-03	[Pim]	8base	Link
2024-04-03	[Innomotive Systems Hainichen GmbH]	raworld	Link
2024-04-03	[Seven Seas Technology]	rhysida	Link
2024-04-01	[casajove.com]	lockbit3	Link
2024-04-03	[delhipolice.gov.in]	killsec	Link
2024-04-02	[regencyfurniture.com]	cactus	Link
2024-04-02	[KICO GROUP]	raworld	Link
2024-04-02	[GRUPOCREATIVO HERRERA]	qilin	Link
2024-04-02	[Fincasrevuelta Data Leak]	everest	Link
2024-04-02	[Precision Pulley & Idler]	blacksuit	Link
2024-04-02	[W.P.J. McCarthy and Company]	qilin	Link
2024-04-02	[Crimsgroup Data Leak]	everest	Link
2024-04-02	[Gaia Herbs]	blacksuit	Link
2024-04-02	[Sterling Plumbing Inc]	raworld	Link
2024-04-02	[C&C Casa e Construção Ltda]	raworld	Link
2024-04-02	[TUBEX Aluminium Tubes]	raworld	Link
2024-04-01	[Roberson & Sons Insurance Services]	qilin	Link
2024-04-01	[Partridge Venture Engineering]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-04-01	[anwaltskanzlei-kaufbeuren.de]	lockbit3	Link
2024-04-01	[pdq-airspares.co.uk]	blackbasta	Link
2024-04-01	[aerodynamicinc.com]	cactus	Link
2024-04-01	[besttrans.com]	cactus	Link
2024-04-01	[Xenwerx Initiatives, LLC]	incransom	Link
2024-04-01	[Blueline Associates]	incransom	Link
2024-04-01	[Sisu Healthcare]	incransom	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.