Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240405

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

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

—

Cisco schließt Sicherheitslücken und gibt Tipps zur VPN-Absicherung

Angreifer können unter anderem WLAN Controller von Cisco attackieren. Tipps gegen Password-Spraying-Attacken sollen VPN-Verbindungen schützen.

- 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-2023-36845	0.966640000	0.996230000	Link
CVE-2023-35082	0.950590000	0.992720000	Link
CVE-2023-30625	0.948330000	0.992380000	Link
CVE-2023-26469	0.938630000	0.990910000	Link
CVE-2023-25194	0.968970000	0.996930000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 04 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

—

Thu, 04 Apr 2024

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

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

- Link

—

Thu, 04 Apr 2024

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Thu, 04 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

—

Thu, 04 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

—

Thu, 04 Apr 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und 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, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.
- Link

—

Thu, 04 Apr 2024

[UPDATE] [hoch] Mozilla Firefox und Firefox ESR: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Thu, 04 Apr 2024

[UPDATE] [hoch] util-linux: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein lokaler Angreifer kann eine Schwachstelle in util-linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Wed, 03 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

—

Wed, 03 Apr 2024

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

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

—

Wed, 03 Apr 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, 03 Apr 2024

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

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

- Link

—

Wed, 03 Apr 2024

[UPDATE] [hoch] Cacti: Mehrere Schwachstellen

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

- Link

—

Wed, 03 Apr 2024

[UPDATE] [hoch] SaltStack Salt: Mehre Schwachstellen

Ein Angreifer kann eine Schwachstelle in SaltStack Salt ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 03 Apr 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Phishing-Angriffe durchzuführen oder Cross-Site Scripting (XSS)-Angriffe auszuführen. Einige dieser Schwachstellen erfordern eine Benutzerinteraktion, um sie erfolgreich auszunutzen.

- Link

—

Wed, 03 Apr 2024

[NEU] [hoch] IBM App Connect Enterprise: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM App Connect Enterprise ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/4/2024	[Debian dsa-5654 : chromium - security update]	critical
4/3/2024	[Fedora 38 : micropython (2024-51e55a7065)]	critical
4/3/2024	[Fedora 39 : micropython (2024-34aa24af35)]	critical
4/3/2024	[Westermo xRD Products Authentication Bypass (CVE-2018-10933)]	critical
4/3/2024	[Westermo WeOS Cryptographic Issues (CVE-2015-7923)]	critical
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
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

Datum	Schwachstelle	Bewertung
4/4/2024	[RHEL 9 : nodejs (RHSA-2024:1678)]	high
4/3/2024	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.5.5.6)]	high
4/3/2024	[Oracle Linux 8 : less (ELSA-2024-1610)]	high
4/3/2024	[Oracle Linux 8 : kernel (ELSA-2024-12266)]	high
4/3/2024	[Oracle Linux 8 : grafana-pcp (ELSA-2024-1644)]	high
4/3/2024	[Oracle Linux 8 : expat (ELSA-2024-1615)]	high
4/3/2024	[Oracle Linux 8 : grafana (ELSA-2024-1646)]	high
4/3/2024	[Oracle Linux 9 : kernel (ELSA-2024-12265)]	high
4/3/2024	[AlmaLinux 8 : grafana (ALSA-2024:1646)]	high
4/3/2024	[AlmaLinux 8 : grafana-pcp (ALSA-2024:1644)]	high
4/3/2024	[Westermo WeOS Stack-Based Buffer Overflow (CVE-2015-7547)]	high
4/3/2024	[Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455 Cross-Site Request Forgery (CSRF) (CVE-2017-12703)]	high
4/3/2024	[Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455 Use of Hard-Coded Cryptographic Key (CVE-2016-5816)]	high
4/3/2024	[Westermo Lynx Code Injection (CVE-2023-45735)]	high
4/3/2024	[Westermo Lynx Cross-Site Request Forgery (CVE-2023-38579)]	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

“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 vul-

nerability 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

—

” “Wed, 03 Apr 2024

ESET NOD32 Antivirus 17.0.16.0 Unquoted Service Path

ESET NOD32 Antivirus version 17.0.16.0 suffers from an unquoted service path vulnerability.

- Link

—

” “Wed, 03 Apr 2024

Computer Laboratory Management System 1.0 SQL Injection

Computer Laboratory Management System version 1.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

” “Tue, 02 Apr 2024

Computer Laboratory Management System 1.0 Cross Site Scripting

Computer Laboratory Management System version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Computer Laboratory Management System 1.0 Insecure Direct Object Reference

Computer Laboratory Management System version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Hospital Management System 1.0 Cross Site Scripting

Hospital Management System version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 02 Apr 2024

PowerVR RGXCreateZSBufferKM2 Use-After-Free

PowerVR has an issue where the RGXCreateZSBufferKM2 error path frees object while on list.

- Link

—

” “Tue, 02 Apr 2024

E-Insurance 1.0 Cross Site Scripting

E-Insurance version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 02 Apr 2024

GL-iNet MT6000 4.5.5 Arbitrary File Download

GL-iNet MT6000 version 4.5.5 suffers from an arbitrary file download vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Rapid7 Nexpose 6.6.240 Unquoted Service Path

Rapid7 Nexpose version 6.6.240 suffers from an unquoted service path vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Blood Bank 1.0 Cross Site Scripting

Blood Bank version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Backdoor.Win32.Agent.ju (PSYRAT) MVID-2024-0677 Bypass / Command Execution

The PsyRAT 0.01 malware listens on random high TCP ports 53297, 53211, 532116 and so forth. Connecting to an infected host returns a logon prompt for PASS. However, you can enter anything or nothing at all and execute commands made available by the backdoor.

- Link

—

” “Tue, 02 Apr 2024

Daily Habit Tracker 1.0 Broken Access Control

Daily Habit Tracker version 1.0 suffers from an access control vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Daily Habit Tracker 1.0 SQL Injection

Daily Habit Tracker version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Daily Habit Tracker 1.0 Cross Site Scripting

Daily Habit Tracker version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Employee Management System 1.0 SQL Injection

Employee Management System version 1.0 suffers from additional remote SQL injection vulnerabilities. Original discovery of this finding is attributed to Ozlem Balci in January of 2024.

- Link

—

” “Tue, 02 Apr 2024

WordPress Simple Backup Path Traversal / Arbitrary File Download

WordPress Simple Backup plugin versions prior to 2.7.10 suffer from file download and path traversal vulnerabilities.

- Link

—

” “Tue, 02 Apr 2024

OpenCart Core 4.0.2.3 SQL Injection

OpenCart Core version 4.0.2.3 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 02 Apr 2024

Online Hotel Booking In PHP 1.0 SQL Injection

Online Hotel Booking in PHP version 1.0 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Tue, 02 Apr 2024

ASUS Control Center Express 01.06.15 Unquoted Service Path

ASUS Control Center Express version 01.06.15 suffers from an unquoted service path vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Mon, 01 Apr 2024

ZDI-24-360: JetBrains TeamCity AgentDistributionSettingsController Cross-Site Scripting Vulnerability

- Link

—

” “Mon, 01 Apr 2024

ZDI-24-359: Flexera Software FlexNet Publisher Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 01 Apr 2024

ZDI-24-358: GitLab Label Description Uncontrolled Resource Consumption Denial-of-Service Vulnerability

- Link

—

” “Mon, 01 Apr 2024

ZDI-24-357: RARLAB WinRAR Mark-Of-The-Web Bypass Vulnerability

- Link

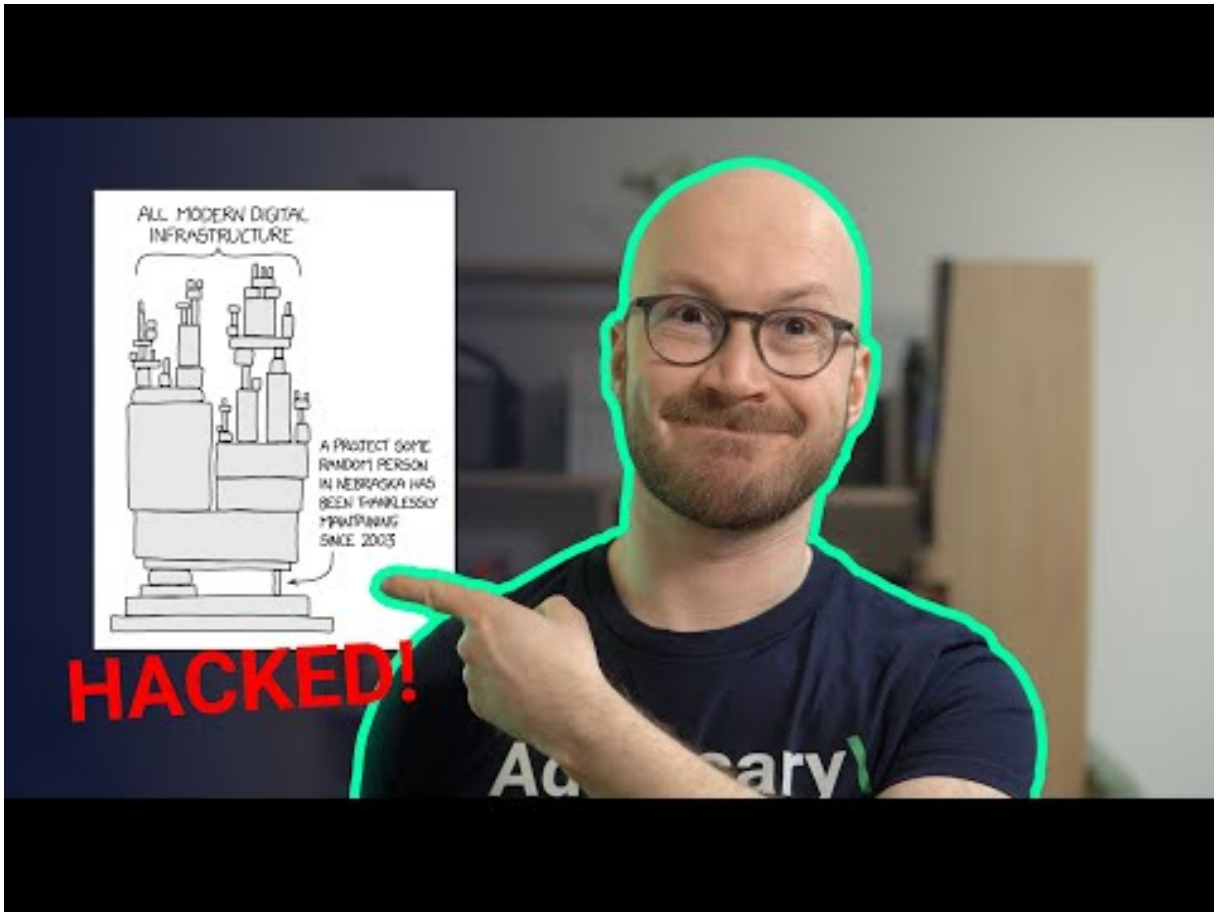
—

”

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
2024-04-07	Comté de Hernando (Hernando County)	[USA]	Link
2024-04-02	Comté de Jackson	[USA]	Link

7 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Grupppe	Webseite
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.