Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240403

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

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

—

Sharepoint-Sicherheitslücken: CISA warnt vor Angriffen in freier Wildbahn

Die CISA warnt vor Angriffen, die auf Sicherheitslücken in Sharepoint beobachtet wurden. Updates gibt es schon länger.

- Link

—

Hintertür in xz-Bibliothek gefährdet SSH-Verbindungen

Der Angriff wurde offenbar von langer Hand geplant. Ein möglicherweise staatlicher Akteur versteckte eine Backdoor in der liblzma-Bibliothek.

- Link

—

Neue SugarCRM-Versionen schließen kritische Lücken

Insgesamt 18, teils kritische Lücken schließen die neuen Versionen SugarCRM 13.03. und 12.05.

- Link

—

Google Chrome: Kritische Schwachstelle bedroht Browser-Nutzer

In Chrome haben Googles Entwickler sieben Sicherheitslücken abgedichtet. Mindestens eine davon stellt ein kritisches Risiko dar.

- Link

—

Loadbalancer: Sicherheitslücken in Loadmaster von Progress/Kemp

In der Loadbalancer-Software Loadmaster von Progress/Kemp klaffen Sicherheitslücken, durch die Angreifer etwa Befehle einschleusen können.

- Link

—

Sicherheitslücken in Microsofts WiX-Installer-Toolset gestopft

Das quelloffene WiX-Installer-Toolset von Microsoft hat zwei Sicherheitslücken. Die dichten aktualisierte Versionen ab.

- Link

—

Firefox: Notfall-Update schließt kritische Sicherheitslücken

Die Mozilla-Entwickler haben zwei kritische Sicherheitslücken mit dem Update auf Firefox 124.0.1 und Firefox ESR 115.9.1 geschlossen.

- Link

—

Kritische Sicherheitslücke in FortiClientEMS wird angegriffen

Eine kritische Schwachstelle in FortiClientEMS wird inzwischen aktiv angegriffen. Zudem ist ein Proof-of-Concept-Exploit öffentlich geworden.

- 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	0.987370000	Link
CVE-2023-6553	0.916210000	0.988470000	Link
CVE-2023-5360	0.967230000	0.996410000	Link
CVE-2023-4966	0.964860000	0.995640000	Link
CVE-2023-47246	0.940270000	0.991060000	Link
CVE-2023-46805	0.964290000	0.995500000	Link
CVE-2023-46747	0.971090000	0.997660000	Link
CVE-2023-46604	0.973060000	0.998590000	Link
CVE-2023-43177	0.927670000	0.989730000	Link
CVE-2023-42793	0.970710000	0.997530000	Link
CVE-2023-39143	0.942940000	0.991410000	Link
CVE-2023-38646	0.928720000	0.989800000	Link
CVE-2023-38203	0.958450000	0.994060000	Link
CVE-2023-38035	0.972180000	0.998170000	Link
CVE-2023-36845	0.966640000	0.996230000	Link
CVE-2023-35813	0.905250000	0.987580000	Link
CVE-2023-3519	0.925380000	0.989450000	Link
CVE-2023-35082	0.950590000	0.992680000	Link
CVE-2023-35078	0.962290000	0.994910000	Link
CVE-2023-34993	0.944980000	0.991800000	Link
CVE-2023-34960	0.935410000	0.990530000	Link
CVE-2023-34634	0.925600000	0.989470000	Link
CVE-2023-34362	0.962490000	0.994960000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.907130000	0.987780000	Link
CVE-2023-3368	0.906550000	0.987690000	Link
CVE-2023-33246	0.973150000	0.998650000	Link
CVE-2023-32315	0.973840000	0.999050000	Link
CVE-2023-32235	0.911650000	0.988140000	Link
CVE-2023-30625	0.948330000	0.992350000	Link
CVE-2023-30013	0.956040000	0.993610000	Link
CVE-2023-29300	0.963460000	0.995240000	Link
CVE-2023-29298	0.926460000	0.989560000	Link
CVE-2023-28771	0.917660000	0.988620000	Link
CVE-2023-28432	0.943220000	0.991470000	Link
CVE-2023-28121	0.938130000	0.990830000	Link
CVE-2023-27524	0.972270000	0.998230000	Link
CVE-2023-27372	0.973490000	0.998890000	Link
CVE-2023-27350	0.972040000	0.998090000	Link
CVE-2023-26469	0.943740000	0.991550000	Link
CVE-2023-26360	0.963570000	0.995260000	Link
CVE-2023-26035	0.969280000	0.997040000	Link
CVE-2023-25717	0.957880000	0.993960000	Link
CVE-2023-25194	0.968970000	0.996930000	Link
CVE-2023-2479	0.963600000	0.995280000	Link
CVE-2023-24489	0.973810000	0.999020000	Link
CVE-2023-23752	0.952140000	0.992930000	Link
CVE-2023-23397	0.923530000	0.989180000	Link
CVE-2023-23333	0.963260000	0.995170000	Link
CVE-2023-22527	0.965680000	0.995990000	Link
CVE-2023-22518	0.970110000	0.997280000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22515	0.971880000	0.998030000	Link
CVE-2023-21839	0.958450000	0.994050000	Link
CVE-2023-21554	0.959700000	0.994320000	Link
CVE-2023-20887	0.964080000	0.995430000	Link
CVE-2023-1671	0.965610000	0.995970000	Link
CVE-2023-0669	0.969540000	0.997120000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 02 Apr 2024

[NEU] [kritisch] xz: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Debian Linux, SUSE Linux, Arch Linux, Fedora Linux, xz und Gentoo Linux ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 02 Apr 2024

[NEU] [hoch] Octopus Deploy: Schwachstelle ermöglicht Privilegieneskalation

Ein authentisierter Angreifer kann eine Schwachstelle in Octopus Deploy ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 02 Apr 2024

[NEU] [hoch] Google Android Patchday April 2024: Mehrere Schwachstellen

Ein anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- Link

—

Tue, 02 Apr 2024

[NEU] [hoch] Imperva SecureSphere: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Imperva SecureSphere ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 02 Apr 2024

[NEU] [hoch] Podman: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- Link

—

Tue, 02 Apr 2024

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

Ein lokaler Angreifer kann eine Schwachstelle in libvirt ausnutzen, um einen Denial of Service Zustand herbeizuführen oder um seine Privilegien zu erhöhen.

- Link

—

Tue, 02 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

—

Tue, 02 Apr 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

—

Tue, 02 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

—

Tue, 02 Apr 2024

[UPDATE] [hoch] Squid: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen

Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link

—

Tue, 02 Apr 2024

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Tue, 02 Apr 2024

[UPDATE] [hoch] Red Hat Advanced Cluster Management for Kubernetes: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Red Hat Advanced Cluster Management for Kubernetes ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Code auszuführen.
- Link

—

Tue, 02 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

—

Tue, 02 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

—

Tue, 02 Apr 2024

[UPDATE] [kritisch] Kemp LoadMaster: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Kemp LoadMaster ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Tue, 02 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

—

Tue, 02 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

—

Tue, 02 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

—

Tue, 02 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

—

Thu, 28 Mar 2024

[NEU] [hoch] SugarCRM Sugar Enterprise: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in SugarCRM Sugar Enterprise ausnutzen, um einen Cross Site Scripting oder einen SQL Injection Angriff durchzuführen, Daten zu manipulieren oder Code auszuführen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/2/2024	[ManageEngine Applications Manager SEoL (10.0.x)]	critical
4/2/2024	[Microsoft Windows 8.1 SEoL]	critical
4/2/2024	[Microsoft Windows Server 2019 SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 IoT Enterprise LTSC SEoL]	critical
4/2/2024	[ManageEngine Applications Manager SEoL (8.0.x)]	critical
4/2/2024	[Microsoft Windows 10 1507 IoT SEoL]	critical
4/2/2024	[Microsoft Windows Server 2012 SEoL]	critical
4/2/2024	[Microsoft Windows 10 1909 Pro SEoL]	critical
4/2/2024	[Microsoft Windows 10 1511 SEoL]	critical
4/2/2024	[Microsoft Windows 10 1607 Enterprise 2016 LTSB SEoL]	critical
4/2/2024	[Microsoft Windows 10 1709 Enterprise SEoL]	critical
4/2/2024	[Microsoft Windows 10 1709 Education SEoL]	critical
4/2/2024	[Microsoft Windows 10 1909 Education SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 Enterprise For Virtual Desktops SEoL]	critical
4/2/2024	[Microsoft Windows 7 SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 Enterprise N SEoL]	critical
4/2/2024	[Microsoft Windows 10 20H2 Education SEoL]	critical
4/2/2024	[Microsoft Windows 10 1507 Home SEoL]	critical
4/2/2024	[Microsoft Windows 10 1803 Education SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 Enterprise Multi Session SEoL]	critical
4/2/2024	[Microsoft Windows 10 1607 Enterprise N SEoL]	critical
4/2/2024	[Microsoft Windows 10 1709 Pro SEoL]	critical
4/2/2024	[ManageEngine Applications Manager SEoL (9.0.x)]	critical
4/2/2024	[Microsoft Windows 10 2004 SEoL]	critical
4/2/2024	[Microsoft Windows 8 SEoL]	critical
4/2/2024	[Microsoft Windows Server 2016 SEoL]	critical
4/2/2024	[Microsoft Windows 10 20H2 Home SEoL]	critical

Datum	Schwachstelle	Bewertung
4/2/2024	[Microsoft Windows 10 1507 Enterprise SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 Enterprise LTSC SEoL]	critical
4/2/2024	[Microsoft Windows 10 1709 Home SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H1 SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 Enterprise SEoL]	critical
4/2/2024	[Microsoft Windows 10 21H2 Pro SEoL]	critical
4/2/2024	[ManageEngine Applications Manager SEoL (11.0.x)]	critical
4/2/2024	[Microsoft Windows 10 1809 Enterprise LTSC SEoL]	critical
4/2/2024	[RHEL 8 : kpatch-patch (RHSA-2024:1612)]	high
4/2/2024	[RHEL 8 : kernel (RHSA-2024:1607)]	high
4/2/2024	[RHEL 8 : less (RHSA-2024:1610)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

—

” “Tue, 02 Apr 2024

Microsoft Windows 10.0.17763.5458 Privilege Escalation

Microsoft Windows version 10.0.17763.5458 kernel IOCTL privilege escalation exploit.

- Link

—

” “Tue, 02 Apr 2024

Elementor Website Builder SQL Injection

Elementor Website Builder versions prior to 3.12.2 suffer from a remote SQL injection vulnerability.

- Link

—

” “Mon, 01 Apr 2024

Packet Storm New Exploits For March, 2024

This archive contains all of the 137 exploits added to Packet Storm in March, 2024.

- Link

—

” “Mon, 01 Apr 2024

ARIS: Business Process Management 10.0.21.0 Cross Site Scripting

ARIS: Business Process Management version 10.0.21.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 01 Apr 2024

Linux nf_tables Local Privilege Escalation

A use-after-free vulnerability exists in the Linux kernel netfilter: nf_tables component. This is a universal local privilege escalation proof of concept exploit working on Linux kernels between 5.14 and 6.6, including Debian, Ubuntu, and KernelCTF.

- Link

—

” “Mon, 01 Apr 2024

BioTime Directory Traversal / Remote Code Execution

BioTime versions 8.5.5 and 9.0.1 suffer from directory traversal and file write vulnerabilities. This exploit also achieves remote code execution on version 8.5.5.

- Link

—

” “Mon, 01 Apr 2024

Gibbon 26.0.00 Server-Side Template Injection / Remote Code Execution

Gibbon version 26.0.00 suffers from a server-side template injection vulnerability that allows for remote code execution.

- Link

—

” “Fri, 29 Mar 2024

WatchGuard XTM Firebox Unauthenticated Remote Command Execution

This Metasploit module exploits a buffer overflow at the administration interface (8080 or 4117) of WatchGuard Firebox and XTM appliances which is built from a cherrypy python backend sending XML-RPC requests to a C binary called wgagent using pre-authentication endpoint /agent/login. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2. Successful exploitation results in remote code execution as user nobody.

- 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

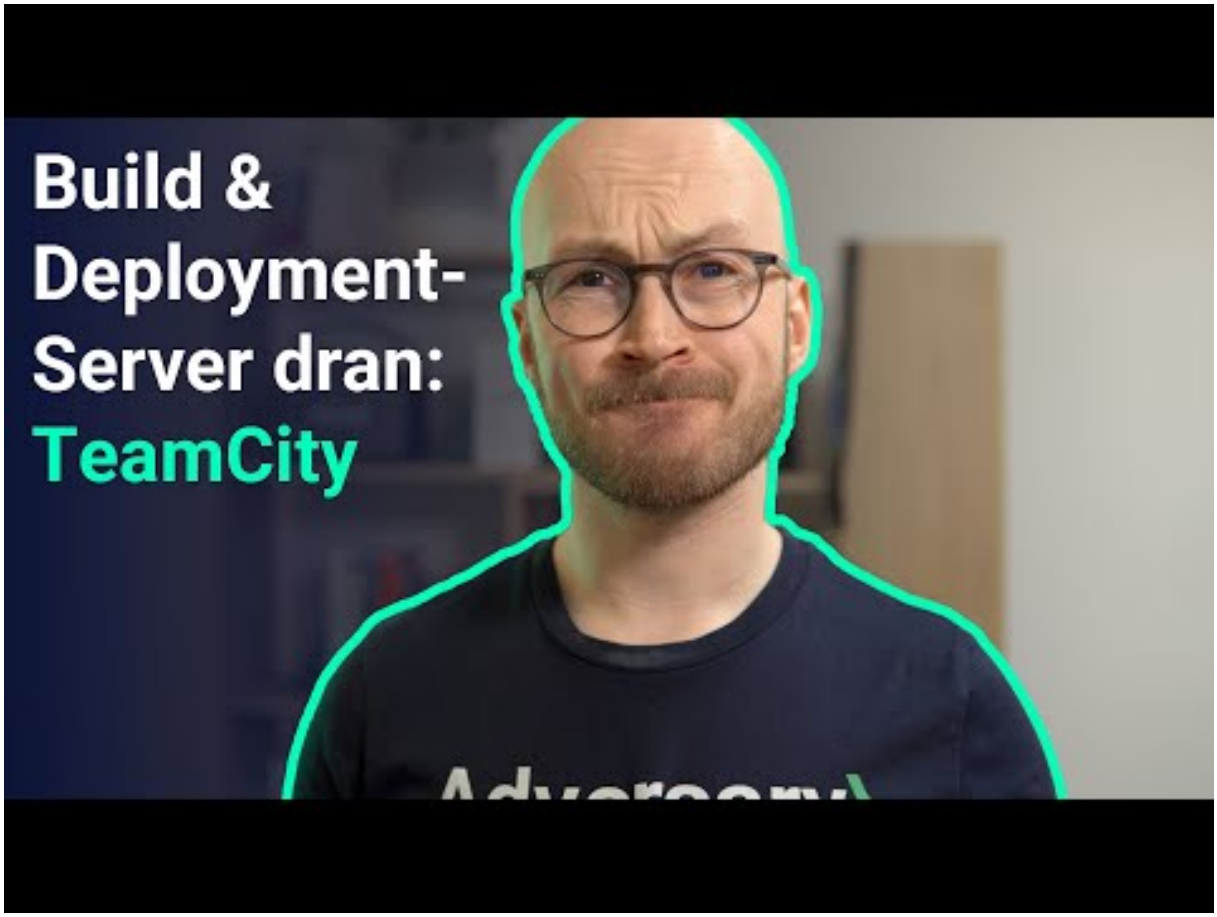
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Hättest du diese Lücke gefunden?



Zum Youtube Video

6 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information

7 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Grupppe	Webseite
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.