Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240402

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

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

—

Microsoft schließt Sicherheitslücke in Xbox-Gaming-Dienst – nach Hickhack

Microsoft hat ein Sicherheitsleck im Xbox Gaming Service abgedichtet. Dem ging jedoch eine Diskussion voraus.

- Link

—

IBM-Software: Angreifer können Systeme mit Schadcode kompromittieren

Es sind wichtige Sicherheitsupdates für IBM App Connect Enterprise und InfoSphere Information Server erschienen.

- Link

—

Lücken in Ruby-Gems ermöglichen Codeschmuggel und Datenleck

Angreifer könnten eigenen Code im Kontext eines Ruby-Programms ausführen. Nutzer der RDoc- und StringIO-Gems sollten aktualisierte Versionen einspielen.

- 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	0.987360000	Link
CVE-2023-6553	0.916210000	0.988460000	Link
CVE-2023-5360	0.967230000	0.996410000	Link
CVE-2023-4966	0.964860000	0.995630000	Link
CVE-2023-47246	0.940270000	0.991050000	Link
CVE-2023-46805	0.964290000	0.995490000	Link
CVE-2023-46747	0.971090000	0.997650000	Link
CVE-2023-46604	0.973060000	0.998600000	Link
CVE-2023-43177	0.927670000	0.989730000	Link
CVE-2023-42793	0.970710000	0.997530000	Link
CVE-2023-39143	0.939910000	0.990990000	Link
CVE-2023-38646	0.928720000	0.989790000	Link
CVE-2023-38203	0.958450000	0.994050000	Link
CVE-2023-38035	0.972180000	0.998170000	Link
CVE-2023-36845	0.966640000	0.996230000	Link
CVE-2023-35813	0.905250000	0.987570000	Link
CVE-2023-3519	0.925380000	0.989440000	Link
CVE-2023-35082	0.932380000	0.990200000	Link
CVE-2023-35078	0.962290000	0.994900000	Link
CVE-2023-34993	0.944980000	0.991800000	Link
CVE-2023-34960	0.935410000	0.990520000	Link
CVE-2023-34634	0.925600000	0.989460000	Link
CVE-2023-34362	0.962490000	0.994940000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.907130000	0.987770000	Link
CVE-2023-3368	0.906550000	0.987690000	Link
CVE-2023-33246	0.973150000	0.998650000	Link
CVE-2023-32315	0.973840000	0.999040000	Link
CVE-2023-32235	0.911650000	0.988140000	Link
CVE-2023-30625	0.948330000	0.992310000	Link
CVE-2023-30013	0.956040000	0.993600000	Link
CVE-2023-29300	0.963460000	0.995230000	Link
CVE-2023-29298	0.926460000	0.989560000	Link
CVE-2023-28771	0.917660000	0.988610000	Link
CVE-2023-28432	0.943220000	0.991460000	Link
CVE-2023-28121	0.938130000	0.990810000	Link
CVE-2023-27524	0.972270000	0.998220000	Link
CVE-2023-27372	0.973490000	0.998890000	Link
CVE-2023-27350	0.972040000	0.998080000	Link
CVE-2023-26469	0.943740000	0.991540000	Link
CVE-2023-26360	0.963570000	0.995260000	Link
CVE-2023-26035	0.969280000	0.997030000	Link
CVE-2023-25717	0.957880000	0.993950000	Link
CVE-2023-25194	0.968970000	0.996930000	Link
CVE-2023-2479	0.963600000	0.995270000	Link
CVE-2023-24489	0.973810000	0.999020000	Link
CVE-2023-23752	0.952140000	0.992920000	Link
CVE-2023-23397	0.923530000	0.989170000	Link
CVE-2023-23333	0.963260000	0.995160000	Link
CVE-2023-22527	0.965680000	0.995980000	Link
CVE-2023-22518	0.970110000	0.997270000	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	0.994310000	Link
CVE-2023-20887	0.964080000	0.995430000	Link
CVE-2023-1671	0.965610000	0.995970000	Link
CVE-2023-0669	0.969540000	0.997110000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 28 Mar 2024

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

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

- Link

—

Thu, 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

—

Thu, 28 Mar 2024

[NEU] [hoch] Cisco IOS XE: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cisco IOS XE ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen, seine Privilegien zu erweitern oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Cisco Aironet Access Point: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Cisco Aironet Access Point, Cisco Catalyst, Cisco Router und Cisco Small Business ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Cisco IOS: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Cisco IOS und Cisco IOS XE ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 28 Mar 2024

[NEU] [UNGEPATCHT] [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] GitLab: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Thu, 28 Mar 2024

[NEU] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um Informationen offenzulegen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] TLS: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in TLS 1.2 ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] python-cryptography: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in python-cryptography ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] dnsmasq: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in dnsmasq ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial of Service Angriff durchzuführen und Sicherheitsmaßnahmen zu umgehen.

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Thu, 28 Mar 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

—

Thu, 28 Mar 2024

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

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

- Link

—

Thu, 28 Mar 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Thu, 28 Mar 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

—

Thu, 28 Mar 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

—

Thu, 28 Mar 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/1/2024	[GLSA-202403-04 : XZ utils: Backdoor in release tarballs]	critical
4/1/2024	[XZ Utils 5.6.0 / 5.6.1 Liblzma Backdoor Check]	critical
3/30/2024	[openSUSE 15 Security Update : minidlna (openSUSE-SU-2024:0093-1)]	critical
3/29/2024	[Linear eMerge Code RCE (CVE-2019-7256)]	critical
3/29/2024	[Potential exposure to XZ Utils SSH Backdoor (CVE-2024-3094)]	critical
4/1/2024	[RHEL 9 : ruby:3.1 (RHSA-2024:1576)]	high
4/1/2024	[FreeBSD : mediawiki – multiple vulnerabilities (d58726ff-ef5e-11ee-8d8e-080027a5b8e9)]	high
3/31/2024	[Debian dsa-5651 : mediawiki - security update]	high
3/31/2024	[Debian dsa-5650 : bsdextrautils - security update]	high
3/31/2024	[Fedora 38 : seamonkey (2024-ad50671f6c)]	high
3/31/2024	[Fedora 39 : seamonkey (2024-8890015ff3)]	high
3/30/2024	[Fedora 39 : cockpit (2024-6065341780)]	high
3/30/2024	[FreeBSD : electron{27,28} – Object lifecycle issue in V8 (bdcd041e-5811-4da3-9243-573a9890fdb1)]	high
3/30/2024	[SUSE SLES15 Security Update : kernel (Live Patch 11 for SLE 15 SP4) (SUSE-SU-2024:1063-1)]	high
3/30/2024	[SUSE SLES15 Security Update : kernel (Live Patch 20 for SLE 15 SP4) (SUSE-SU-2024:1072-1)]	high
3/30/2024	[Fedora 39 : suricata (2024-99337cc4a1)]	high
3/30/2024	[Fedora 38 : suricata (2024-34eba1b1a6)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 7 for SLE 15 SP5) (SUSE-SU-2024:1040-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 40 for SLE 15 SP3) (SUSE-SU-2024:1033-1)]	high

Datum	Schwachstelle	Bewertung
3/29/2024	[SUSE SLES12 Security Update : kernel (Live Patch 48 for SLE 12 SP5) (SUSE-SU-2024:1028-1)]	high
3/29/2024	[SUSE SLES15 Security Update : podman (SUSE-SU-2024:1059-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 5 for SLE 15 SP5) (SUSE-SU-2024:1045-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 41 for SLE 15 SP3) (SUSE-SU-2024:1054-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 31 for SLE 15 SP3) (SUSE-SU-2024:1047-1)]	high
3/29/2024	[SUSE SLES15 Security Update : kernel (Live Patch 43 for SLE 15 SP2) (SUSE-SU-2024:1053-1)]	high
3/29/2024	[SUSE SLES15 Security Update : podman (SUSE-SU-2024:1058-1)]	high
3/29/2024	[ForgeRock Access Management 7.2.0 / 7.1.x < 7.1.4 / 7.0.x <= 7.0.2 Path Traversal]	high
3/29/2024	[Security Updates for Microsoft Office Products C2R (March 2024)]	high
3/29/2024	[Atlassian Confluence < 7.19.20 / 7.20.x < 8.5.7 (CONFSERVER-94843)]	high
3/29/2024	[Curl 7.44.0 < 8.7.0 HTTP/2 Push Headers Memory-leak (CVE-2024-2398)]	high
3/29/2024	[Curl 8.6.0 < 8.7.0 QUIC Certificate Check Bypass (CVE-2024-2379)]	high
3/29/2024	[Curl 8.5.0 < 8.7.0 TLS Certificate Check Bypass (CVE-2024-2466)]	high
3/29/2024	[F5 Networks BIG-IP : DNS vulnerability (K000139092)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“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

WordPress Gutenberg 18.0.0 Cross Site Scripting

WordPress Gutenberg plugin version 18.0.0 suffers from a persistent cross site scripting vulnerability.

- 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

—

” “Fri, 29 Mar 2024

Soholaunch 4.9.4 r44 Shell Upload

Soholaunch version 4.9.4 r44 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 29 Mar 2024

FoF Pretty Mail 1.1.2 Local File Inclusion

The FoF Pretty Mail extension version 1.1.2 for Flarum suffers from a local file inclusion vulnerability.

- Link

—

” “Fri, 29 Mar 2024

FoF Pretty Mail 1.1.2 Server-Side Template Injection

The FoF Pretty Mail extension version 1.1.2 for Flarum suffers from a server-side template injection vulnerability.

- Link

—

” “Fri, 29 Mar 2024

FoF Pretty Mail 1.1.2 Command Injection

The FoF Pretty Mail extension version 1.1.2 for Flarum suffers from a command injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Event Management 1.0 SQL Injection

Event Management version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

util-linux wall Escape Sequence Injection

The util-linux wall command does not filter escape sequences from command line arguments. The vulnerable code was introduced in commit cdd3cc7fa4 (2013). Every version since has been vulnerable. This allows unprivileged users to put arbitrary text on other users terminals, if mesg is set to y and wall is setgid. CentOS is not vulnerable since wall is not setgid. On Ubuntu 22.04 and Debian Bookworm, wall is both setgid and mesg is set to y by default.

- Link

—

” “Thu, 28 Mar 2024

Circontrol Raption Buffer Overflow / Command Injection

The server in Circontrol Raption versions through 5.11.2 has a pre-authentication stack-based buffer overflow that can be exploited to gain run-time control of the device as root. The pwrstudio web application of EV Charger (in the server in Circontrol Raption through 5.6.2) is vulnerable to OS command injection.

- Link

—

” “Thu, 28 Mar 2024

FusionPBX Session Fixation

FusionPBX suffers from a session fixation vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Dell Security Management Server Privilege Escalation

Dell Security Management Server versions prior to 11.9.0 suffer from a local privilege escalation vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Purei CMS 1.0 SQL Injection

Purei CMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Workout Journal App 1.0 Cross Site Scripting

Workout Journal App version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 28 Mar 2024

LMS PHP 1.0 SQL Injection

LMS PHP version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 28 Mar 2024

Asterisk AMI 18.20.0 File Content / Path Disclosure

Asterisk AMI version 18.20.0 suffers from authenticated partial file content and path disclosure vulnerabilities.

- Link

—

” “Thu, 28 Mar 2024

Siklu MultiHaul TG Series Credential Disclosure

Siklu MultiHaul TG Series versions prior to 2.0.0 suffer from an unauthenticated credential disclosure vulnerability.

- Link

—

” “Thu, 28 Mar 2024

RouterOS 6.44 / 6.49.10 Denial Of Service

RouterOS versions 6.40.5 through 6.44 and 6.48.1 through 6.49.10 suffers from a denial of service vulnerability.

- Link

—

” “Thu, 28 Mar 2024

NodeBB 3.6.7 Broken Access Control

NodeBB version 3.6.7 suffers from a broken access control that lets attackers via data only meant for an administrator.

- Link

—

” “Thu, 28 Mar 2024

WinRAR 6.22 Remote Code Execution

WinRAR version 6.22 suffers from a remote code execution vulnerability via a malicious zip archive.

- Link

—

” “Wed, 27 Mar 2024

Sharepoint Dynamic Proxy Generator Remote Command Execution

This Metasploit module exploits two vulnerabilities in Sharepoint 2019 - an authentication bypass as noted in CVE-2023-29357 which was patched in June of 2023 and CVE-2023-24955 which was a remote command execution vulnerability patched in May of 2023. The authentication bypass allows attackers to impersonate the Sharepoint Admin user. This vulnerability stems from the signature va-

lidation check used to verify JSON Web Tokens (JWTs) used for OAuth authentication. If the signing algorithm of the user-provided JWT is set to none, SharePoint skips the signature validation step due to a logic flaw in the ReadTokenCore() method. After impersonating the administrator user, the attacker has access to the Sharepoint API and is able to exploit CVE-2023-24955. This authenticated remote command execution vulnerability leverages the impersonated privileged account to replace the /BusinessDataMetadataCatalog/BDCMetadata.bdcm file in the webroot directory with a payload. The payload is then compiled and executed by Sharepoint allowing attackers to remotely execute commands via the API.

- 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

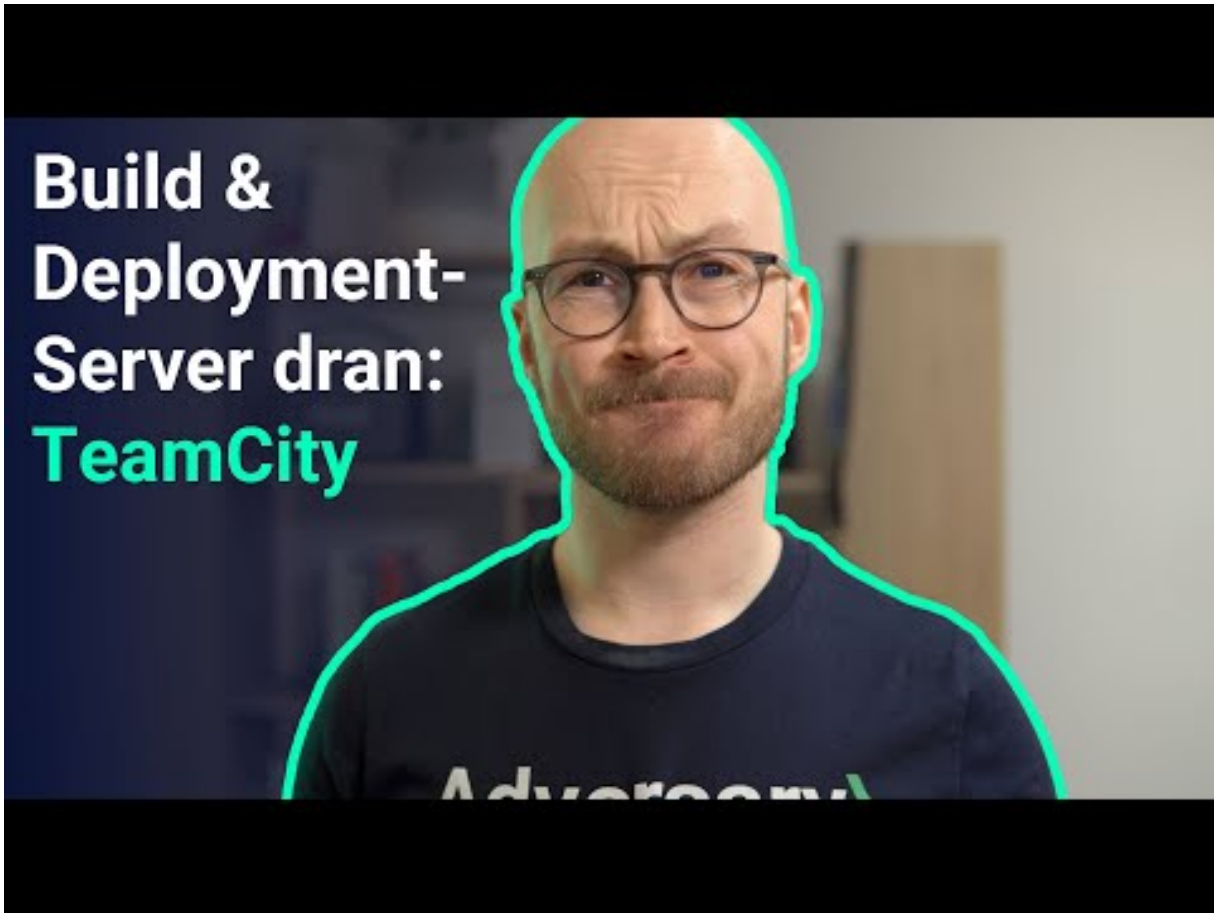
—

”

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
2024-04-02	[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.