Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240317

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

HP: Viele Laptops und PCs von Codeschmuggel-Lücke betroffen

Eine BIOS-Sicherheitsfunktion von HP-Laptops und -PCs kann von Angreifern umgangen werden. BIOS-Updates stehen bereit oder werden grad entwickelt.

- Link

—

Cisco schließt hochriskante Lücken in IOS XR

Cisco warnt vor SIcherheitslücken mit teils hohem Risiko im Router-Betriebssystem IOS XR. Updates stehen bereit.

- Link

—

Fortinet-Patchday: Updates gegen kritische Schwachstellen

Fortinet hat zum März-Patchday Sicherheitslücken in FortiOS, FortiProxy, FortiClientEMS und im FortiManager öffentlich gemacht.

- Link

—

Adobe-Patchday: Angreifer können verwundbare Systeme übernehmen

Adobe stopft am März-Patchday teils kritische Sicherheitslücken in sechs Produkten. Sie erlauben unter anderem Codeschmuggel.

- Link

—

Microsoft Patchday: Hersteller stopft 59 Sicherheitslücken

Der März-Patchday von Microsoft ist etwas weniger umfangreich: 59 Sicherheitslecks haben die Entwickler gestopft.

- Link

—

Google Chrome: Lücke erlaubte Codeschmuggel

Google schließt drei Sicherheitslücken im Webbrowser Chrome. Mindestens eine gilt als hochriskant, Angreifer könnten Schadcode dadurch einschleusen.

- Link

—

Synology: Update schließt “wichtige” Lücken in Synology Router Manager

Im Synology Router Manager (SRM) klaffen Sicherheitslecks, durch die Angreifer etwa Scripte einschleusen können. Ein Update steht bereit.

- Link

—

SAP schließt zehn Sicherheitslücken am März-Patchday

SAP hat zehn neue Sicherheitsmitteilungen zum März-Patchday veröffentlicht. Zwei der geschlossenen Lücken gelten als kritisch.

- Link

—

ArubaOS: Sicherheitslücken erlauben Befehlsschmuggel

HPE Aruba hat eine Sicherheitsmitteilung zu mehreren Lücken herausgegeben. Angreifer können Befehle einschleusen oder einen DoS auslösen.

- Link

—

Qnap hat teils kritische Lücken in seinen Betriebssystemen geschlossen

Qnap hat Warnungen vor Sicherheitslücken in QTS, QuTS Hero und QuTScloud veröffentlicht. Aktualisierte Firmware dichtet sie ab.

- 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	0.987170000	Link
CVE-2023-5360	0.967230000	0.996350000	Link
CVE-2023-4966	0.966110000	0.996030000	Link
CVE-2023-47246	0.943540000	0.991450000	Link
CVE-2023-46747	0.972020000	0.998050000	Link
CVE-2023-46604	0.973060000	0.998600000	Link
CVE-2023-43177	0.927670000	0.989620000	Link
CVE-2023-42793	0.970930000	0.997570000	Link
CVE-2023-39143	0.933560000	0.990220000	Link
CVE-2023-38646	0.916640000	0.988400000	Link
CVE-2023-38205	0.934710000	0.990350000	Link
CVE-2023-38203	0.959860000	0.994260000	Link
CVE-2023-38035	0.972370000	0.998280000	Link
CVE-2023-36845	0.966580000	0.996140000	Link
CVE-2023-3519	0.911860000	0.987990000	Link
CVE-2023-35082	0.935540000	0.990430000	Link
CVE-2023-35078	0.963380000	0.995120000	Link
CVE-2023-34960	0.929930000	0.989800000	Link
CVE-2023-34634	0.919000000	0.988640000	Link
CVE-2023-34362	0.960450000	0.994460000	Link
CVE-2023-34039	0.901300000	0.987140000	Link
CVE-2023-3368	0.904650000	0.987370000	Link
CVE-2023-33246	0.973410000	0.998820000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32315	0.973840000	0.999050000	Link
CVE-2023-32235	0.905760000	0.987440000	Link
CVE-2023-30625	0.946250000	0.991810000	Link
CVE-2023-30013	0.945460000	0.991720000	Link
CVE-2023-29300	0.963690000	0.995210000	Link
CVE-2023-29298	0.921360000	0.988860000	Link
CVE-2023-28771	0.922340000	0.988970000	Link
CVE-2023-28432	0.941310000	0.991080000	Link
CVE-2023-28121	0.929770000	0.989760000	Link
CVE-2023-27524	0.972240000	0.998210000	Link
CVE-2023-27372	0.971320000	0.997760000	Link
CVE-2023-27350	0.971970000	0.998030000	Link
CVE-2023-26469	0.937680000	0.990680000	Link
CVE-2023-26360	0.960730000	0.994530000	Link
CVE-2023-26035	0.970030000	0.997200000	Link
CVE-2023-25717	0.962180000	0.994770000	Link
CVE-2023-2479	0.962540000	0.994860000	Link
CVE-2023-24489	0.973400000	0.998820000	Link
CVE-2023-23752	0.948570000	0.992220000	Link
CVE-2023-23397	0.917330000	0.988470000	Link
CVE-2023-23333	0.963260000	0.995080000	Link
CVE-2023-22518	0.970110000	0.997220000	Link
CVE-2023-22515	0.971880000	0.997990000	Link
CVE-2023-21839	0.960490000	0.994470000	Link
CVE-2023-21554	0.959700000	0.994220000	Link
CVE-2023-20887	0.965070000	0.995680000	Link
CVE-2023-1671	0.961560000	0.994630000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-0669	0.968640000	0.996770000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 15 Mar 2024

[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Fri, 15 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

—

Fri, 15 Mar 2024

[UPDATE] [hoch] binutils: Mehrere Schwachstellen

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

- Link

—

Fri, 15 Mar 2024

[NEU] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Dateien zu manipulieren oder Informationen offenzulegen.

- Link

—

Thu, 14 Mar 2024

[NEU] [hoch] Arcserve Unified Data Protection: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Arcserve Unified Data Protection ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service zu verursachen.
- Link

—

Thu, 14 Mar 2024

[NEU] [hoch] IBM Maximo Asset Management: Mehrere Schwachstellen

Ein anonymer Angreifer kann mehrere Schwachstellen in IBM Maximo Asset Management ausnutzen, um Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen oder einen Cross-Site-Scripting-Angriff (XSS) durchzuführen.
- Link

—

Thu, 14 Mar 2024

[UPDATE] [hoch] Microsoft Windows: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Windows ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder Infor mationen offenzulegen.
- Link

—

Thu, 14 Mar 2024

[NEU] [hoch] JFrog Artifactory: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in JFrog Artifactory ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.
- Link

—

Thu, 14 Mar 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

Thu, 14 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, 14 Mar 2024

[UPDATE] [hoch] vim: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und Dateien zu manipulieren.

- Link

—

Thu, 14 Mar 2024

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

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder unbekannte Auswirkungen zu verursachen.

- Link

—

Thu, 14 Mar 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, 14 Mar 2024

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

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

- Link

—

Thu, 14 Mar 2024

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Thu, 14 Mar 2024

[UPDATE] [hoch] Microsoft Visual Studio 2022: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um einen Denial of Service Angriff durchzuführen oder seine Privilegien zu erweitern.

- Link

—

Thu, 14 Mar 2024

[NEU] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen ermöglichen Manipulation von

Dateien

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 13 Mar 2024

[UPDATE] [hoch] Android Patchday Juni 2022

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand auszulösen.

- Link

—

Wed, 13 Mar 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

—

Wed, 13 Mar 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/15/2024	[Progress OpenEdge 11.7.x < 11.7.19 / 12.2.x < 12.2.13 / 12.8.x < 12.8.1 (000253075)]	critical
3/15/2024	[Mobatek MobaXterm < 8.3 (CVE-2015-7244)]	critical

Datum	Schwachstelle	Bewertung
3/15/2024	[Mobatek MobaXterm < 22.3 (CVE-2022-38337)]	critical
3/15/2024	[Mobatek MobaXterm 11.1 u3860 (CVE-2019-7690)]	critical
3/15/2024	[Mobatek MobaXterm 10.4 (CVE-2017-15376)]	critical
3/15/2024	[Debian dla-3762 : unadf - security update]	critical
3/16/2024	[openSUSE 15 Security Update : python-rpyc (openSUSE-SU-2024:0082-1)]	high
3/16/2024	[SUSE SLES12 Security Update : sudo (SUSE-SU-2024:0890-1)]	high
3/16/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:0900-2)]	high
3/16/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:0910-1)]	high
3/16/2024	[SUSE SLES15 Security Update : sudo (SUSE-SU-2024:0889-1)]	high
3/16/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:0893-1)]	high
3/15/2024	[Oracle Linux 8 : .NET / 8.0 (ELSA-2024-1311)]	high
3/15/2024	[Oracle Linux 9 : .NET / 8.0 (ELSA-2024-1310)]	high
3/15/2024	[Oracle Linux 9 : .NET / 7.0 (ELSA-2024-1309)]	high
3/15/2024	[SUSE SLES15 Security Update : vim (SUSE-SU-2024:0871-1)]	high
3/15/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gdb (SUSE-SU-2024:0898-1)]	high
3/15/2024	[SUSE SLES15 Security Update : sudo (SUSE-SU-2024:0877-1)]	high
3/15/2024	[SUSE SLES15 Security Update : kernel (SUSE-SU-2024:0900-1)]	high
3/15/2024	[SUSE SLES12 Security Update : fontforge (SUSE-SU-2024:0863-1)]	high
3/15/2024	[SUSE SLES15 Security Update : gdb (SUSE-SU-2024:0899-1)]	high

Datum	Schwachstelle	Bewertung
3/15/2024	[openSUSE 15 Security Update : python-Django (SUSE-SU-2024:0902-1)]	high
3/15/2024	[Microsoft Azure Data Studio < 1.48.0 Elevation of Privilege Vulnerability (CVE-2024-26203)]	high
3/15/2024	[Security Updates for Microsoft Exchange Server (March 2024)]	high
3/15/2024	[Adobe Lightroom 0.0.x < 7.2 (apsb24-17)]	high
3/15/2024	[Mobatek MobaXterm < 21.0 (CVE-2021-28847)]	high
3/15/2024	[Mobatek MobaXterm 11.1 / 12.1 (CVE-2019-16305)]	high
3/15/2024	[Mobatek MobaXterm 11.1 (CVE-2019-13475)]	high
3/15/2024	[Mobatek MobaXterm < 22.2 (CVE-2022-38336)]	high
3/15/2024	[Oracle Linux 8 : dnsmasq (ELSA-2024-1335)]	high
3/15/2024	[Oracle Linux 9 : dnsmasq (ELSA-2024-1334)]	high
3/15/2024	[Fedora 39 : iwd (2024-4ef5edfb2a)]	high
3/15/2024	[Fedora 38 : chromium (2024-ac1eb810c5)]	high
3/15/2024	[Oracle Linux 8 : .NET / 7.0 (ELSA-2024-1308)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Fri, 15 Mar 2024

Financials By Coda Authorization Bypass

Financials by Coda versions prior to 2023Q4 suffer from an incorrect access control authorization bypass vulnerability. The Change Password feature can be abused in order to modify the password of any user of the application.

- Link

—

” “Fri, 15 Mar 2024

Financials By Coda Cross Site Scripting

Financials by Coda versions prior to 2023Q4 suffer from a cross site scripting vulnerability.

- Link

—

” “Fri, 15 Mar 2024

HALO 2.13.1 CORS Issue

HALO version 2.13.1 has an insecure cross-origin resource sharing setting that allows an arbitrary origin.

- Link

—

” “Fri, 15 Mar 2024

Membership Management System 1.0 SQL Injection / Shell Upload

Membership Management System version 1.0 suffers from remote shell upload and remote SQL injection vulnerabilities.

- Link

—

” “Thu, 14 Mar 2024

Checkmk Agent 2.0.0 / 2.1.0 / 2.2.0 Local Privilege Escalation

Checkmk Agent versions 2.0.0, 2.1.0, and 2.2.0 suffer from a local privilege escalation vulnerability.

- Link

—

” “Thu, 14 Mar 2024

Vinchin Backup And Recovery 7.2 Command Injection

Vinchin Backup and Recovery versions 7.2 and below suffer from an authentication command injection vulnerability.

- Link

—

” “Thu, 14 Mar 2024

Fortinet FortiOS Out-Of-Bounds Write

Fortinet FortiOS suffers from an out of bounds write vulnerability. Affected includes Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, and 1.0.0 through 1.0.7.

- Link

—

” “Thu, 14 Mar 2024

JetBrains TeamCity Unauthenticated Remote Code Execution

This Metasploit module exploits an authentication bypass vulnerability in JetBrains TeamCity. An unauthenticated attacker can leverage this to access the REST API and create a new administrator access token. This token can be used to upload a plugin which contains a Metasploit payload, allowing

the attacker to achieve unauthenticated remote code execution on the target TeamCity server. On older versions of TeamCity, access tokens do not exist so the exploit will instead create a new administrator account before uploading a plugin. Older versions of TeamCity have a debug endpoint (/app/rest/debug/process) that allows for arbitrary commands to be executed, however recent version of TeamCity no longer ship this endpoint, hence why a plugin is leveraged for code execution instead, as this is supported on all versions tested.

- Link

—

” “Thu, 14 Mar 2024

Backdoor.Win32.Emegrab.b MVID-2024-0675 Buffer Overflow

Backdoor.Win32.Emegrab.b malware suffers from a buffer overflow vulnerability.

- Link

—

” “Thu, 14 Mar 2024

StimulusReflex 3.5.0 Arbitrary Code Execution

StimulusReflex versions 3.5.0 up to and including 3.5.0.rc2 and 3.5.0.pre10 suffer from an arbitrary code execution vulnerability.

- Link

—

” “Thu, 14 Mar 2024

GitLab CE/EE Password Reset

GitLab CE/EE versions prior to 16.7.2 suffer from a password reset vulnerability.

- Link

—

” “Thu, 14 Mar 2024

JetBrains TeamCity 2023.05.3 Remote Code Execution

JetBrains TeamCity version 2023.05.3 suffers from a remote code execution vulnerability.

- Link

—

” “Thu, 14 Mar 2024

Honeywell PM43 Remote Code Execution

Honeywell PM43 versions prior to P10.19.050004 suffer from a remote code execution vulnerability.

- Link

—

” “Thu, 14 Mar 2024

SolarView Compact 6.00 Command Injection

SolarView Compact version 6.00 suffers from a remote command injection vulnerability.

- Link

—

” “Thu, 14 Mar 2024

Viessmann Vitogate 300 2.1.3.0 Remote Code Execution

Viessmann Vitogate 300 versions 2.1.3.0 and below suffers from a remote code execution vulnerability.

- Link

—

” “Thu, 14 Mar 2024

Ruijie Switch PSG-5124 26293 Remote Code Execution

Ruijie Switch version PSG-5124 with software build 26293 suffers from a remote code execution vulnerability.

- Link

—

” “Wed, 13 Mar 2024

Stealing Part Of A Production Language Model

In this whitepaper, the authors introduce the first model-stealing attack that extracts precise, nontrivial information from black-box production language models like OpenAI’s ChatGPT or Google’s PaLM-2. Specifically, their attack recovers the embedding projection layer (up to symmetries) of a transformer model, given typical API access. For under $20 USD, their attack extracts the entire projection matrix of OpenAI’s ada and babbage language models. They thereby confirm, for the first time, that these black-box models have a hidden dimension of 1024 and 2048, respectively. They also recover the exact hidden dimension size of the gpt-3.5-turbo model, and estimate it would cost under $2,000 in queries to recover the entire projection matrix. They conclude with potential defenses and mitigations, and discuss the implications of possible future work that could extend this attack.

- Link

—

” “Wed, 13 Mar 2024

Client Details System 1.0 SQL Injection

Client Details System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 13 Mar 2024

MetaFox 5.1.8 Shell Upload

MetaFox versions 5.1.8 and below suffer from a remote shell upload vulnerability.

- Link

—

” “Wed, 13 Mar 2024

Cisco Firepower Management Center Remote Command Execution

Cisco Firepower Management Center suffers from an authenticated remote command execution vulnerability. Many versions spanning the 7.x.x.x and 6.x.x.x branches are affected.
- Link

—

” “Wed, 13 Mar 2024

SnipeIT 6.2.1 Cross Site Scripting

SnipeIT version 6.2.1 suffers from a persistent cross site scripting vulnerability.
- Link

—

” “Wed, 13 Mar 2024

MSMS-PHP 1.0 Shell Upload

MSMS-PHP version 1.0 suffers from a remote shell upload vulnerability.
- Link

—

” “Wed, 13 Mar 2024

MSMS-PHP 1.0 SQL Injection

MSMS-PHP version 1.0 suffers from a remote SQL injection vulnerability.
- Link

—

” “Wed, 13 Mar 2024

VMware Cloud Director 10.5 Authentication Bypass

VMware Cloud Director version 10.5 suffers from an authentication bypass vulnerability.
- Link

—

” “Wed, 13 Mar 2024

Karaf 4.4.3 Remote Code Execution

Karaf version 4.4.3 suffers from a remote code execution vulnerability.
- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 13 Mar 2024

ZDI-24-294: Microsoft Office Performance Monitor Link Following Local Privilege Escalation Vulnerability
- Link

—

” “Wed, 13 Mar 2024

ZDI-24-293: Microsoft Skype Protection Mechanism Failure Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Mar 2024

ZDI-24-292: Adobe Premiere Pro AVI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 13 Mar 2024

ZDI-24-291: Adobe Bridge PS File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

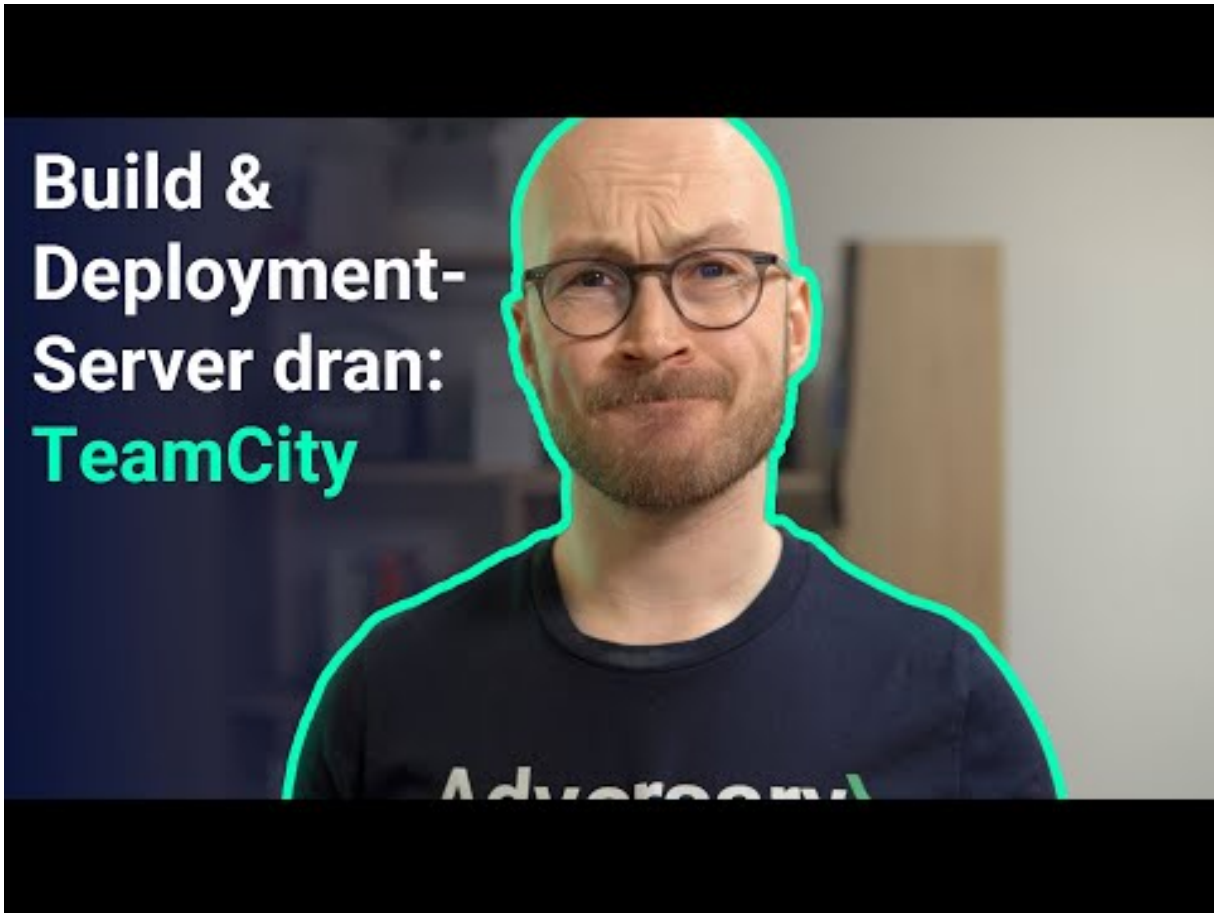
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Hättest du diese Lücke gefunden?



Zum Youtube Video

6 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2024-03-14	NHS Dumfries and Galloway	[GBR]	Link
2024-03-14	Scranton School District	[USA]	Link
2024-03-13	Maxis	[MYS]	Link
2024-03-10	edpnet	[BEL]	Link
2024-03-10	Town of Huntsville	[CAN]	Link
2024-03-10	MarineMax	[USA]	Link
2024-03-09	Leicester City Council	[GBR]	Link
2024-03-08	Kärntner Landesversicherung (KLV)	[AUT]	Link
2024-03-07	Administradora de Subsidios Sociales (ADESS)	[DOM]	Link
2024-03-07	Beyers Koffie	[BEL]	Link
2024-03-06	Brasserie Duvel Moortgat	[BEL]	Link
2024-03-06	Nisqually Red Wind Casino	[USA]	Link
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	Link
2024-03-04	South St. Paul Public Schools	[USA]	Link
2024-03-01	Hansab	[EST]	Link

7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-16	[Indoarsip]	trigona	Link
2024-03-16	[Bwizer]	trigona	Link
2024-03-16	[Topa Partners]	trigona	Link
2024-03-16	[HUDSONBUSSALES.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-15	[Desco Steel]	medusa	Link
2024-03-15	[Metzger Veterinary Services]	medusa	Link
2024-03-16	[Consolidated Benefits Resources]	bianlian	Link
2024-03-16	[agribank.com.na]	lockbit3	Link
2024-03-16	[triella.com]	lockbit3	Link
2024-03-16	[rrib.com]	lockbit3	Link
2024-03-16	[newmans-online.co.uk]	lockbit3	Link
2024-03-16	[hdstrading.com]	lockbit3	Link
2024-03-16	[duttonbrock.com]	lockbit3	Link
2024-03-16	[colefabrics.com]	lockbit3	Link
2024-03-16	[bergmeister.eu]	lockbit3	Link
2024-03-16	[automotionshade.com]	lockbit3	Link
2024-03-16	[Miki Travel]	hunters	Link
2024-03-16	[certifiedcollection.com]	lockbit3	Link
2024-03-16	[Acculabs Inc]	incransom	Link
2024-03-08	[oyaksgs.com.tr]	lockbit3	Link
2024-03-15	[elezabypharmacy.com]	lockbit3	Link
2024-03-15	[South St Paul Public Schools]	blacksuit	Link
2024-03-12	[ATL Leasing]	hunters	Link
2024-03-14	[lostlb]	stormous	Link
2024-03-14	[education.eeb-lost]	stormous	Link
2024-03-14	[worthenind.com]	lockbit3	Link
2024-03-14	[rushenergyservices.com]	lockbit3	Link
2024-03-14	[sbmandco.com]	lockbit3	Link
2024-03-14	[mckimcreed.com]	lockbit3	Link
2024-03-14	[moperry.com]	lockbit3	Link
2024-03-14	[Cosmocolor]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-14	[voidinteractive.net you are welcome in our chat]	donutleaks	Link
2024-03-14	[journeyfreight.com]	lockbit3	Link
2024-03-14	[dhanisisd.net]	lockbit3	Link
2024-03-14	[mioa.gov]	stormous	Link
2024-03-14	[gfad.de]	blackbasta	Link
2024-03-14	[Keboda Technology Co., Ltd.]	bianlian	Link
2024-03-14	[iamdesign.com]	abyss	Link
2024-03-14	[yarco.com]	abyss	Link
2024-03-13	[McKim & Creed]	ransomhub	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Summit Almonds]	akira	Link
2024-03-13	[Encina Wastewater Authority]	blackbyte	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Felda Global Ventures Holdings Berhad]	qilin	Link
2024-03-13	[geruestbau.com]	lockbit3	Link
2024-03-13	[Judge Rotenberg Center]	blacksuit	Link
2024-03-12	[Dörr Group]	snatch	Link
2024-03-13	[Kovra]	ransomhub	Link
2024-03-13	[Brewer Davidson]	8base	Link
2024-03-13	[Forstinger Österreich GmbH]	8base	Link
2024-03-04	[vsexshop.ru]	werewolves	Link
2024-03-11	[QEO Group]	play	Link
2024-03-12	[ATL]	hunters	Link
2024-03-12	[duvel.com	boulevard.com]	blackbasta
2024-03-11	[Kenneth Young Center]	medusa	Link
2024-03-12	[sunholdings.net]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-12	[xcelbrands.com]	blackbasta	Link
2024-03-12	[cpacsystems.se]	blackbasta	Link
2024-03-12	[elmatic.de]	blackbasta	Link
2024-03-12	[keystonetech.com]	blackbasta	Link
2024-03-12	[dutyfreeamericas.com]	blackbasta	Link
2024-03-12	[sierralobo.com]	blackbasta	Link
2024-03-12	[contechs.co.uk]	blackbasta	Link
2024-03-12	[creativeenvironments.com]	blackbasta	Link
2024-03-12	[linksunlimited.com]	blackbasta	Link
2024-03-12	[imperialtrading.com]	blackbasta	Link
2024-03-12	[Brooks Tropicals]	rhysida	Link
2024-03-12	[Withall]	blacksuit	Link
2024-03-12	[WALKERSANDFORD]	blacksuit	Link
2024-03-12	[Kaplan]	hunters	Link
2024-03-06	[Sprimoglass]	8base	Link
2024-03-11	[Schokinag]	play	Link
2024-03-11	[Zips Car Wash]	play	Link
2024-03-11	[Bechtold]	play	Link
2024-03-11	[Canada Revenue Agency]	play	Link
2024-03-11	[White Oak Partners]	play	Link
2024-03-11	[Ruda Auto]	play	Link
2024-03-11	[Image Pointe]	play	Link
2024-03-11	[Grassmid Transport]	play	Link
2024-03-11	[Fashion UK]	play	Link
2024-03-11	[QI Group]	play	Link
2024-03-11	[BiTec]	play	Link
2024-03-11	[Bridger Insurance]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-11	[SREE Hotels]	play	Link
2024-03-11	[Q?? ??o??]	play	Link
2024-03-11	[Premier Technology]	play	Link
2024-03-11	[londonvisionclinic.com]	lockbit3	Link
2024-03-11	[lec-london.uk]	lockbit3	Link
2024-03-11	[Computan]	ransomhub	Link
2024-03-11	[plymouth.com]	cactus	Link
2024-03-11	[neigc.com]	abyss	Link
2024-03-11	[gpaa.gov.za]	lockbit3	Link
2024-03-11	[NetVigour]	hunters	Link
2024-03-11	[cleshar.co.uk]	cactus	Link
2024-03-11	[ammega.com]	cactus	Link
2024-03-11	[renypicot.es]	cactus	Link
2024-03-11	[Scadea Solutions]	ransomhub	Link
2024-03-09	[https://www.consorzioinnova.it]	alphalocker	Link
2024-03-09	[DVT]	ransomhub	Link
2024-03-09	[Rekamy]	ransomhub	Link
2024-03-09	[go4kora]	ransomhub	Link
2024-03-09	[H + G EDV Vertriebs]	blacksuit	Link
2024-03-09	[Fincasrevuelta]	everest	Link
2024-03-09	[Lindsay Municipal Hospital]	bianlian	Link
2024-03-09	[Group Health Cooperative - Rev 500kk]	blacksuit	Link
2024-03-09	[ACE Air Cargo]	hunters	Link
2024-03-09	[Watsonclinic.com]	donutleaks	Link
2024-03-06	[Continental Aerospace Technologies]	play	Link
2024-03-08	[redwoodcoastrc.org]	lockbit3	Link
2024-03-08	[PowerRail Distribution]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-08	[Denninger's]	medusa	Link
2024-03-08	[SIEA]	ransomhub	Link
2024-03-08	[Hozzify]	ransomhub	Link
2024-03-07	[rmhfranchise.com]	lockbit3	Link
2024-03-07	[New York Home Healthcare]	bianlian	Link
2024-03-07	[Palmer Construction Co., Inc]	bianlian	Link
2024-03-07	[en-act-architecture]	qilin	Link
2024-03-07	[Merchant ID]	ransomhub	Link
2024-03-07	[SP Mundi]	ransomhub	Link
2024-03-07	[www.duvel.com]	stormous	Link
2024-03-06	[www.loghmanpharma.com]	stormous	Link
2024-03-06	[MainVest]	play	Link
2024-03-06	[C?????????? A???????e T???????????]	play	Link
2024-03-05	[Haivision MCS]	medusa	Link
2024-03-06	[Tocci Building Corporation]	medusa	Link
2024-03-06	[JVCKENWOOD]	medusa	Link
2024-03-06	[American Renal Associates]	medusa	Link
2024-03-06	[US #1364 Federal Credit Union]	medusa	Link
2024-03-06	[viadirectamarketing]	stormous	Link
2024-03-06	[Liquid Environmental Solutions]	incransom	Link
2024-03-06	[Infosoft]	akira	Link
2024-03-06	[brightwires.com.sa]	qilin	Link
2024-03-06	[Medical Billing Specialists]	akira	Link
2024-03-06	[Telecentro]	akira	Link
2024-03-06	[Steiner (Austrian furniture makers)]	akira	Link
2024-03-06	[Biomedical Research Institute]	meow	Link
2024-03-06	[K???o???]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-06	[Kudulis Reisinger Price]	8base	Link
2024-03-06	[Global Zone]	8base	Link
2024-03-06	[Mediplast AB]	8base	Link
2024-03-05	[airbogo]	stormous	Link
2024-03-05	[sunwave.com.cn]	lockbit3	Link
2024-03-05	[SJCME.EDU]	clop	Link
2024-03-05	[central.k12.or.us]	lockbit3	Link
2024-03-05	[iemsc.com]	qilin	Link
2024-03-05	[hawita-gruppe]	qilin	Link
2024-03-05	[Future Generations Foundation]	meow	Link
2024-03-04	[Seven Seas Group]	snatch	Link
2024-03-04	[Paul Davis Restoration]	medusa	Link
2024-03-04	[Veeco]	medusa	Link
2024-03-04	[dismogas]	stormous	Link
2024-03-04	[everplast]	stormous	Link
2024-03-04	[DiVal Safety Equipment, Inc.]	hunters	Link
2024-03-04	[America Chung Nam orACN]	akira	Link
2024-03-03	[jovani.com]	lockbit3	Link
2024-03-03	[valoremreply.com]	lockbit3	Link
2024-03-04	[Martin’s, Inc.]	bianlian	Link
2024-03-03	[Prompt Financial Solutions]	medusa	Link
2024-03-03	[Sophiahemmet University]	medusa	Link
2024-03-03	[Centennial Law Group LLP]	medusa	Link
2024-03-03	[Eastern Rio Blanco Metropolitan]	medusa	Link
2024-03-03	[Chris Argiropoulos Professional]	medusa	Link
2024-03-03	[THAISUMMIT.US]	clop	Link
2024-03-03	[THESAFIRCHOICE.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-03	[ipmaltamira]	alphv	Link
2024-03-03	[earnesthealth.com]	lockbit3	Link
2024-03-03	[Ward Transport & Logistics]	dragonforce	Link
2024-03-03	[Ponoka.ca]	cloak	Link
2024-03-03	[stockdevelopment.com]	lockbit3	Link
2024-03-03	[Ewig Usa]	alphv	Link
2024-03-02	[aerospace.com]	lockbit3	Link
2024-03-02	[starkpower.de]	lockbit3	Link
2024-03-02	[roehr-stolberg.de]	lockbit3	Link
2024-03-02	[schuett-grundei.de]	lockbit3	Link
2024-03-02	[unitednotions.com]	lockbit3	Link
2024-03-02	[smuldes.com]	lockbit3	Link
2024-03-02	[esser-ps.de]	lockbit3	Link
2024-03-01	[SBM & Co [You have 48 hours. Check your e-mail]]	alphv	Link
2024-03-01	[Skyland Grain]	play	Link
2024-03-01	[American Nuts]	play	Link
2024-03-01	[A&A Wireless]	play	Link
2024-03-01	[Powill Manufacturing & Engineering]	play	Link
2024-03-01	[Trans+Plus Systems]	play	Link
2024-03-01	[Hedlunds]	play	Link
2024-03-01	[Red River Title]	play	Link
2024-03-01	[Compact Mould]	play	Link
2024-03-01	[Winona Pattern & Mold]	play	Link
2024-03-01	[Marketon]	play	Link
2024-03-01	[Stack Infrastructure]	play	Link
2024-03-01	[Coastal Car]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-01	[New Bedford Welding Supply]	play	Link
2024-03-01	[Influence Communication]	play	Link
2024-03-01	[Kool-air]	play	Link
2024-03-01	[FBi Construction]	play	Link
2024-03-01	[SBM & Co]	alphv	Link
2024-03-01	[Shooting House]	ransomhub	Link
2024-03-01	[Crystal Window & Door Systems]	dragonforce	Link
2024-03-01	[Gilmore Construction]	blacksuit	Link
2024-03-01	[Petrus Resources Ltd]	alphv	Link
2024-03-01	[CoreData]	akira	Link
2024-03-01	[Gansevoort Hotel Group]	akira	Link
2024-03-01	[DJI Company]	mogilevich	Link
2024-03-01	[Kick]	mogilevich	Link
2024-03-01	[Shein]	mogilevich	Link
2024-03-01	[Kumagai Gumi Group]	alphv	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.