Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240612

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

SAP liefert am Patchday Sicherheitskorrekturen für zwei hochriskante Lücken

SAP warnt zum Juni-Patchday vor zehn neuen Sicherheitslücken. Aktualisierungen zum Abdichten der Lecks stehen bereit.

- Link

—

Schwachstelle in PyTorch erlaubt Command Injection via RPC auf dem Master Node

Eine Schwachstelle in dem Machine-Learning-Framework ermöglicht beim verteilten Training das Ausführen beliebigem Code auf dem Master Node.

- Link

—

Sicherheitspatch nachgebessert: Schadcode-Attacken auf PHP möglich

Angreifer können unter Windows den Schutz für eine PHP-Sicherheitslücke aus 2012 umgehen. Eigentlich sollte die Lücke längst geschlossen sein.

- Link

—

Kritische Azure-Lücke: Patch-Status derzeit unklar

Microsofts Cloud-Computing-Plattform Azure ist attackierbar. Sicherheitsforschern zufolge können Angreifer Schadcode auf Endpoints von Kunden ausführen.

- Link

—

Jetzt patchen! Exploitcode für kritische Lücke in Apache HugeGraph in Umlauf

Admins sollten aus Sicherheitsgründen das Tool zum Erstellen von Diagrammen HugeGraph von Apache zügig auf den aktuellen Stand bringen.

- Link

—

Kritische DoS-Lücke bedroht IBM App Connect Enterprise Certified Container

Angreifer könnten IBM App Connect Enterprise Certified Container und DesignerAuthoring attackieren.

- Link

—

Sicherheitsupdates trotz Supportende: Zyxel sichert NAS-Systeme ab

Offensichtlich sind fünf jüngst entdeckte Lücken derart gefährlich, dass Zyxel sich um die EoL-Geräte kümmern muss.

- Link

—

Patchday: Attacken auf Geräte mit Android 12, 13 und 14 möglich

Wichtige Sicherheitsupdates schließen mehrere Schwachstellen in verschiedenen Android-Versionen.

- Link

—

IT-Management-Plattform SolarWinds über mehrere Wege angreifbar

Die SolarWinds-Entwickler haben mehrere Sicherheitslücken in ihrer Software geschlossen. Angreifer können etwa für Abstürze sorgen.

- Link

—

Sicherheitsupdate: Schadcode-Attacken auf Autodesk AutoCAD möglich

Die CAD-Softwares Advance Steel, Civil 3D und AutoCAD von Autodesk sind verwundbar. Das Sicherheitsrisiko gilt als hoch.

- 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-2023-7028	0.959520000	0.994730000	Link
CVE-2023-6553	0.918870000	0.989290000	Link
CVE-2023-5360	0.911260000	0.988700000	Link
CVE-2023-4966	0.969240000	0.997220000	Link
CVE-2023-48795	0.961680000	0.995170000	Link
CVE-2023-47246	0.935450000	0.991030000	Link
CVE-2023-46805	0.955460000	0.994050000	Link
CVE-2023-46747	0.971460000	0.998060000	Link
CVE-2023-46604	0.931360000	0.990630000	Link
CVE-2023-4542	0.924200000	0.989820000	Link
CVE-2023-43208	0.963060000	0.995470000	Link
CVE-2023-43177	0.960230000	0.994880000	Link
CVE-2023-42793	0.970430000	0.997600000	Link
CVE-2023-41265	0.914120000	0.988910000	Link
CVE-2023-39143	0.948440000	0.992870000	Link
CVE-2023-38646	0.900980000	0.987970000	Link
CVE-2023-38205	0.938000000	0.991320000	Link
CVE-2023-38203	0.968530000	0.997040000	Link
CVE-2023-38146	0.905210000	0.988250000	Link
CVE-2023-38035	0.975020000	0.999830000	Link
CVE-2023-36845	0.966630000	0.996420000	Link
CVE-2023-3519	0.909250000	0.988520000	Link
CVE-2023-35082	0.967870000	0.996830000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968250000	0.996960000	Link
CVE-2023-34993	0.971450000	0.998050000	Link
CVE-2023-34960	0.922740000	0.989600000	Link
CVE-2023-34634	0.923550000	0.989690000	Link
CVE-2023-34468	0.900570000	0.987940000	Link
CVE-2023-34362	0.957100000	0.994320000	Link
CVE-2023-34039	0.944630000	0.992220000	Link
CVE-2023-3368	0.928050000	0.990230000	Link
CVE-2023-33246	0.972320000	0.998440000	Link
CVE-2023-32315	0.973460000	0.998950000	Link
CVE-2023-32235	0.902790000	0.988100000	Link
CVE-2023-30625	0.950680000	0.993220000	Link
CVE-2023-30013	0.963050000	0.995470000	Link
CVE-2023-29300	0.969840000	0.997410000	Link
CVE-2023-29298	0.943950000	0.992070000	Link
CVE-2023-28771	0.918640000	0.989270000	Link
CVE-2023-28121	0.932700000	0.990780000	Link
CVE-2023-27524	0.970620000	0.997670000	Link
CVE-2023-27372	0.973630000	0.999030000	Link
CVE-2023-27350	0.971140000	0.997900000	Link
CVE-2023-26469	0.942400000	0.991840000	Link
CVE-2023-26360	0.952190000	0.993490000	Link
CVE-2023-26035	0.967700000	0.996790000	Link
CVE-2023-25717	0.956860000	0.994270000	Link
CVE-2023-25194	0.967930000	0.996860000	Link
CVE-2023-2479	0.963670000	0.995660000	Link
CVE-2023-24489	0.973550000	0.998990000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.944080000	0.992100000	Link
CVE-2023-23397	0.922480000	0.989570000	Link
CVE-2023-23333	0.963260000	0.995530000	Link
CVE-2023-22527	0.972960000	0.998680000	Link
CVE-2023-22518	0.961970000	0.995230000	Link
CVE-2023-22515	0.973130000	0.998770000	Link
CVE-2023-21839	0.959090000	0.994650000	Link
CVE-2023-21554	0.955760000	0.994090000	Link
CVE-2023-20887	0.965950000	0.996250000	Link
CVE-2023-20198	0.915340000	0.989020000	Link
CVE-2023-1698	0.912990000	0.988800000	Link
CVE-2023-1671	0.969090000	0.997170000	Link
CVE-2023-0669	0.968870000	0.997120000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 11 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.

- Link

—

Tue, 11 Jun 2024

[NEU] [hoch] JetBrains Produkte: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IntelliJ IDEA, DataGrip, PhpStorm, PyCharm und WebStorm IDEA ausnutzen, um Informationen offenzulegen.

- Link

—

Tue, 11 Jun 2024

[NEU] [hoch] Siemens SIMATIC S7: Schwachstelle ermöglicht Denial of Service und Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Siemens SIMATIC S7 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen und Informationen offenzulegen.

- Link

—

Tue, 11 Jun 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- Link

—

Tue, 11 Jun 2024

[UPDATE] [hoch] win.rar WinRAR: Schwachstelle ermöglicht Denial of Service und Informationsoffenlegung

Ein Angreifer kann eine Schwachstelle in win.rar WinRAR ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Informationen offenlegen.

- Link

—

Tue, 11 Jun 2024

[NEU] [hoch] VLC: Schwachstelle ermöglicht Denial of Service

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

- Link

—

Tue, 11 Jun 2024

[NEU] [UNGEPATCHT] [kritisch] PyTorch: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Tue, 11 Jun 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Tue, 11 Jun 2024

[NEU] [hoch] SAP Software: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen, um seine Privilegien zu erhöhen, Cross-Site-Scripting (XSS)-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- Link

—

Tue, 11 Jun 2024

[NEU] [hoch] Red Hat Enterprise Linux (FreeIPA): Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um seine Privilegien zu erhöhen, Dateien zu manipulieren und vertrauliche Informationen offenzulegen.

- Link

—

Tue, 11 Jun 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

—

Tue, 11 Jun 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Tue, 11 Jun 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

—

Tue, 11 Jun 2024

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode

auszuführen, seine Privilegien zu erweitern, einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- Link

—

Tue, 11 Jun 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- Link

—

Tue, 11 Jun 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

—

Tue, 11 Jun 2024

[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Tue, 11 Jun 2024

[UPDATE] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern oder vertrauliche Informationen offenzulegen.

- Link

—

Tue, 11 Jun 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 oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Tue, 11 Jun 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Komponenten von Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/11/2024	[Google Chrome < 126.0.6478.56 Multiple Vulnerabilities]	critical
6/11/2024	[Google Chrome < 126.0.6478.56 Multiple Vulnerabilities]	critical
6/11/2024	[Adobe FrameMaker Publishing Server 2022 < 17.3.0.0 (2022.3.0.0) Privilege Escalation (APSB24-38)]	critical
6/11/2024	[KB5039227: Windows 2022 / Azure Stack HCI 22H2 Security Update (June 2024)]	critical
6/11/2024	[KB5039294: Windows Server 2012 R2 Security Update (June 2024)]	critical
6/11/2024	[KB5039225: Windows 10 LTS 1507 Security Update (June 2024)]	critical
6/11/2024	[KB5039266: Windows Server 2008 Security Update (June 2024)]	critical
6/11/2024	[KB5039213: Windows 11 version 21H2 Security Update (June 2024)]	critical
6/11/2024	[KB5039211: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (June 2024)]	critical
6/11/2024	[KB5039260: Windows Server 2012 Security Update (June 2024)]	critical

Datum	Schwachstelle	Bewertung
6/11/2024	[KB5039212: Windows 11 version 22H2 / Windows 11 version 23H2 Security Update (June 2024)]	critical
6/11/2024	[KB5039274: Windows Server 2008 R2 Security Update (June 2024)]	critical
6/11/2024	[KB5039217: Windows 10 version 1809 / Windows Server 2019 Security Update (June 2024)]	critical
6/11/2024	[KB5039214: Windows 10 Version 1607 / Windows Server 2016 Security Update (June 2024)]	critical
6/11/2024	[KB5039236: Windows 11 version 22H2 / Windows Server version 23H2 Security Update (June 2024)]	critical
6/11/2024	[Slackware Linux 15.0 / current mozilla-firefox Multiple Vulnerabilities (SSA:2024-163-01)]	critical
6/11/2024	[Fortinet Fortigate (FG-IR-23-460)]	high
6/11/2024	[RHEL 8 : kpatch-patch (RHSA-2024:3805)]	high
6/11/2024	[AlmaLinux 9 : booth (ALSA-2024:3661)]	high
6/11/2024	[AlmaLinux 8 : booth (ALSA-2024:3659)]	high
6/11/2024	[Security Updates for Microsoft SharePoint Server Subscription Edition (June 2024)]	high
6/11/2024	[Security Updates for Microsoft SharePoint Server 2016 (June 2024)]	high
6/11/2024	[Security Updates for Microsoft SharePoint Server 2019 (June 2024)]	high
6/11/2024	[Security Updates for Microsoft Office Products (June 2024)]	high
6/11/2024	[Security Updates for Outlook (June 2024)]	high
6/11/2024	[Security Updates for Microsoft Visual Studio Products (June 2024)]	high
6/11/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : mod_jk vulnerability (USN-6826-1)]	high
6/11/2024	[Fortinet Fortigate (FG-IR-24-036)]	high
6/11/2024	[Amazon Linux 2 : firefox (ALASFIREFOX-2024-025)]	high

Datum	Schwachstelle	Bewertung
6/11/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-071)]	high
6/11/2024	[Debian dsa-5707 : libvlc-bin - security update]	high
6/11/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-3784)]	high
6/11/2024	[Ubuntu 22.04 LTS : Linux kernel (NVIDIA) vulnerabilities (USN-6820-2)]	high
6/11/2024	[Ubuntu 20.04 LTS : Linux kernel (Intel IoTG) vulnerabilities (USN-6828-1)]	high
6/11/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (AWS) vulnerabilities (USN-6821-3)]	high
6/11/2024	[Ubuntu 23.10 : Linux kernel vulnerabilities (USN-6819-2)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 11 Jun 2024

VSCode ipynb Remote Code Execution

VSCode when opening a Jupyter notebook (.ipynb) file bypasses the trust model. On versions v1.4.0 through v1.71.1, its possible for the Jupyter notebook to embed HTML and javascript, which can then open new terminal windows within VSCode. Each of these new windows can then execute arbitrary code at startup. During testing, the first open of the Jupyter notebook resulted in pop-ups displaying errors of unable to find the payload exe file. The second attempt at opening the Jupyter notebook would result in successful execution. Successfully tested against VSCode 1.70.2 on Windows 10.

- Link

—

” “Tue, 11 Jun 2024

Oracle Database Password Hash Unauthorized Access

Oracle Database versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, and 19c allows for unauthorized access to password hashes by an account with the DBA role.

- Link

—

” “Mon, 10 Jun 2024

Kiuwan Local Analyzer / SAST / SaaS XML Injection / XSS / IDOR

Kiuwan SAST versions prior to 2.8.2402.3, Kiuwan Local Analyzer versions prior to master.1808.p685.q13371, and Kiuwan SaaS versions prior to 2024-02-05 suffer from XML external entity injection, cross site scripting, insecure direct object reference, and various other vulnerabilities.

- Link

—

” “Mon, 10 Jun 2024

SEH utnserver Pro/ProMAX / INU-100 20.1.22 XSS / DoS / File Disclosure

SEH utnserver Pro/ProMAX and INU-100 version 20.1.22 suffers from cross site scripting, denial of service, and file disclosure vulnerabilities.

- Link

—

” “Mon, 10 Jun 2024

FengOffice 3.11.1.2 SQL Injection

FengOffice version 3.11.1.2 suffers from a remote blind SQL injection vulnerability.

- Link

—

” “Fri, 07 Jun 2024

Online Pizza Ordering System 1.0 SQL Injection

Online Pizza Ordering System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 07 Jun 2024

Apache HugeGraph Remote Command Execution

Apache HugeGraph versions 1.0.0 and up to 1.3.0 suffer from a remote command execution vulnerability. This is a scanner to test for the issue.

- Link

—

” “Thu, 06 Jun 2024

Boelter Blue System Management 1.3 SQL Injection

Boelter Blue System Management version 1.3 suffers from a remote SQL injection vulnerability.

- Link

—

” “Thu, 06 Jun 2024

Trojan.Win32.DarkGateLoader MVID-2024-0685 Code Execution

Multiple variants of Trojan.Win32.DarkGateLoader malware suffer from a code execution vulnerability.

- Link

—

” “Thu, 06 Jun 2024

Small CRM 1.0 SQL Injection

Small CRM version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Thu, 06 Jun 2024

Small CRM 1.0 Cross Site Scripting

Small CRM version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Thu, 06 Jun 2024

Northwind Demo 1.0 Cross Site Scripting

Northwind Demo version 1.0 suffers from persistent cross site scripting vulnerability.

- Link

—

” “Thu, 06 Jun 2024

WordPress Hash Form 1.1.0 Remote Code Execution

The Hash Form Drag and Drop Form Builder plugin for WordPress suffers from a critical vulnerability due to missing file type validation in the file_upload_action function. This vulnerability exists in all versions up to and including 1.1.0. Unauthenticated attackers can exploit this flaw to upload arbitrary files, including PHP scripts, to the server, potentially allowing for remote code execution on the affected WordPress site. This Metasploit module targets multiple platforms by adapting payload delivery and execution based on the server environment.

- Link

—

” “Tue, 04 Jun 2024

PowerVR DevmemXIntMapPages() Mapping Issue

PowerVR suffers from an issue where DevmemXIntMapPages() allows mapping sDevZeroPage/sDummyPage without holding reference.

- Link

—

” “Mon, 03 Jun 2024

Check Point Security Gateway Arbitrary File Read Detection Tool

This is a vulnerability detection and exploitation tool design to take in a list of targets and check for the arbitrary file read vulnerability in Check Point Security Gateways.

- Link

—

” “Mon, 03 Jun 2024

Check Point Security Gateway Arbitrary File Read

Proof of concept exploit for Check Point Security Gateways that allows an unauthenticated remote attacker to read the contents of an arbitrary file located on the affected appliance.

- Link

—

” “Mon, 03 Jun 2024

Employee And Visitor Gate Pass Logging System 1.0 SQL Injection

Employee and Visitor Gate Pass Logging System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 03 Jun 2024

FreePBX 16 Remote Code Execution

FreePBX suffers from a remote code execution vulnerability. Versions 14, 15, and 16 are all affected.

- Link

—

” “Mon, 03 Jun 2024

Sitefinity 15.0 Cross Site Scripting

Sitefinity version 15.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 03 Jun 2024

appRain CMF 4.0.5 Shell Upload

appRain CMF version 4.0.5 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 03 Jun 2024

CMSimple 5.15 Remote Shell Upload

CMSimple version 5.15 suffers from a remote shell upload vulnerability.

- Link

—

” “Mon, 03 Jun 2024

Monstra CMS 3.0.4 Remote Code Execution

Monstra CMS version 3.0.4 suffers from a remote code execution vulnerability. Original discovery of code execution in this version is attributed to Ishaq Mohammed in December of 2017.

- Link

—

” “Mon, 03 Jun 2024

Dotclear 2.29 Remote Code Execution

Dotclear version 2.29 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 03 Jun 2024

WBCE CMS 1.6.2 Remote Code Execution

WBCE CME version 1.6.2 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 03 Jun 2024

Serendipity 2.5.0 Remote Code Execution

Serendipity version 2.5.0 suffers from a remote code execution vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 11 Jun 2024

ZDI-24-600: Schneider Electric APC Easy UPS Online startRun Exposed Dangerous Method Remote Code Execution Vulnerability

- Link

—

” “Tue, 11 Jun 2024

ZDI-24-599: Adobe Substance 3D Stager SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Tue, 11 Jun 2024

ZDI-24-598: (0Day) Microsoft Windows Incorrect Permission Assignment Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-597: Centreon initCurveList SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-596: Centreon updateServiceHost_MC SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-595: Centreon updateServiceHost SQL Injection Remote Code Execution Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-594: Siemens Tecnomatix Plant Simulation MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-593: Linux Kernel Net Scheduler Out-Of-Bounds Access Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-592: Linux Kernel nftables Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-591: Linux Kernel RSVP Filter Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-590: Linux Kernel ksmbd smb2_open Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-589: Linux Kernel ksmbd Read Request Memory Leak Denial-of-Service Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-588: Linux Kernel ksmbd Read Request Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-587: Linux Kernel ksmbd SetInfo Request Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-586: Linux Kernel ksmbd Transform Header Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-585: Trend Micro VPN Proxy One Pro Link Following Denial-of-Service Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-584: (Pwn2Own) NETGEAR RAX30 fing_dil Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 10 Jun 2024

ZDI-24-583: (Pwn2Own) NETGEAR RAX30 Improper Certificate Validation Remote Code Execution Vulnerability

- Link

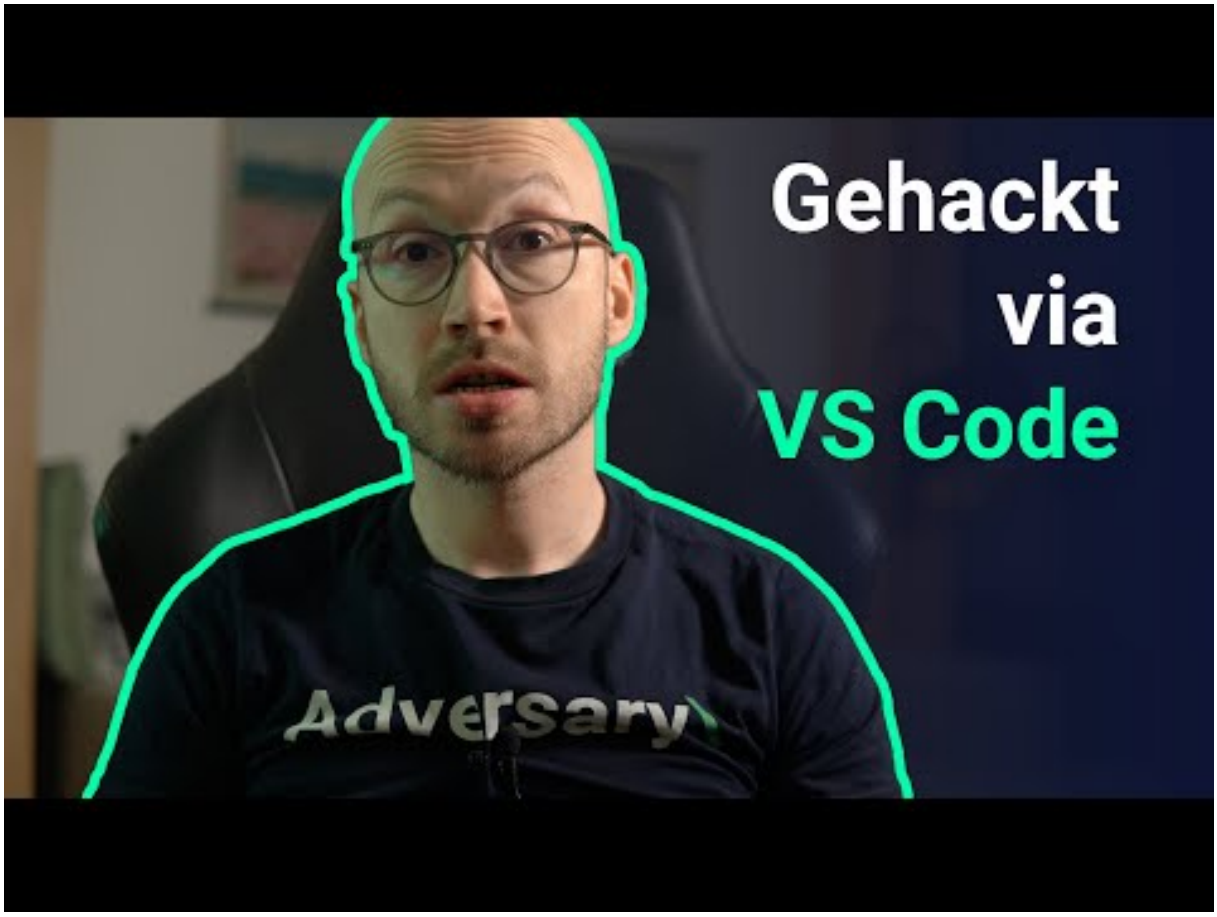
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Die nächste Wahnsinns-Möglichkeit für Angreifer, Software-Unternehmen zu hacken (VSCode Extensions)



Zum Youtube Video

6 Cyberangriffe: (Jun)

Datum	Opfer	Land	Information
2024-06-09	Cleveland	[USA]	Link
2024-06-09	Hands, The Family Network	[CAN]	Link
2024-06-09	Emcali	[COL]	Link
2024-06-08	KADOKAWA	[JPN]	Link
2024-06-08	Mobile County Health Department	[USA]	Link
2024-06-08	Findlay Automotive Group	[USA]	Link
2024-06-06	ASST Rhodense	[ITA]	Link
2024-06-04	Vietnam Post Corporation (Vietnam Post)	[VNM]	Link
2024-06-04	Synnovis	[GBR]	Link
2024-06-04	Groupe IPM	[BEL]	Link
2024-06-02	Institut technologique de Sonora (Itson)	[MEX]	Link

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-06	[filmetrics corporation]	trinity	Link
2024-06-11	[Embotits Espina, SLU]	8base	Link
2024-06-10	[a-agroup]	qilin	Link
2024-06-10	[Harper Industries]	hunters	Link
2024-06-10	[nordspace.lt]	darkvault	Link
2024-06-05	[www.ugrocapital.com]	ransomhub	Link
2024-06-10	[Arge Baustahl]	akira	Link
2024-06-10	[transportlaberge.com]	cactus	Link
2024-06-10	[sanyo-shokai.co.jp]	cactus	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-10	[wave2.co.kr]	darkvault	Link
2024-06-10	[jmthompson.com]	cactus	Link
2024-06-10	[ctsystem.com]	cactus	Link
2024-06-10	[ctgbrands.com]	cactus	Link
2024-06-10	[SolidCAM]	handala	Link
2024-06-08	[EvoEvents]	dragonforce	Link
2024-06-08	[Barrett Eye Care]	dragonforce	Link
2024-06-08	[Parrish-McCall Constructors]	dragonforce	Link
2024-06-08	[California Rice Exchange]	rhysida	Link
2024-06-07	[Allied Toyota Lift]	qilin	Link
2024-06-08	[Hoppecke]	dragonforce	Link
2024-06-07	[Elite Limousine Plus Inc]	bianlian	Link
2024-06-07	[ccmaui.org]	lockbit3	Link
2024-06-07	[talalayglobal.com]	blackbasta	Link
2024-06-07	[akdenizchemson.com]	blackbasta	Link
2024-06-07	[Reinhold Sign Service]	akira	Link
2024-06-07	[Axip Energy Services]	hunters	Link
2024-06-06	[RAVEN Mechanical]	hunters	Link
2024-06-06	[dmedelivers.com]	embargo	Link
2024-06-06	[fpr-us.com]	cactus	Link
2024-06-06	[TBMCG.com]	ElDorado	Link
2024-06-06	[www.vet.k-state.edu]	ElDorado	Link
2024-06-06	[www.uccretrievals.com]	ElDorado	Link
2024-06-06	[robson.com]	blackbasta	Link
2024-06-06	[elutia.com]	blackbasta	Link
2024-06-06	[ssiworld.com]	blackbasta	Link
2024-06-06	[driver-group.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-06	[HTE Technologies]	ElDorado	Link
2024-06-06	[goughhomes.com]	ElDorado	Link
2024-06-06	[Baker Triangle]	ElDorado	Link
2024-06-06	[www.tankerska.hr]	ElDorado	Link
2024-06-06	[cityofpensacola.com]	ElDorado	Link
2024-06-06	[thunderbirdcc.org]	ElDorado	Link
2024-06-06	[www.itasnatta.edu.it]	ElDorado	Link
2024-06-06	[panzersolutions.com]	ElDorado	Link
2024-06-06	[lindostar.it]	ElDorado	Link
2024-06-06	[burotec.biz]	ElDorado	Link
2024-06-06	[celplan.com]	ElDorado	Link
2024-06-06	[adamshomes.com]	ElDorado	Link
2024-06-06	[dynasafe.com]	blackbasta	Link
2024-06-06	[Panasonic Australia]	akira	Link
2024-06-04	[Health People]	medusa	Link
2024-06-04	[IPPBX]	medusa	Link
2024-06-04	[Market Pioneer International Corp]	medusa	Link
2024-06-04	[Mercy Drive Inc]	medusa	Link
2024-06-04	[Radiosurgery New York]	medusa	Link
2024-06-04	[Inside Broadway]	medusa	Link
2024-06-04	[Oracle Advisory Services]	medusa	Link
2024-06-04	[Women’s Sports Foundation]	medusa	Link
2024-06-05	[“Moshe Kahn Advocates”]	mallox	Link
2024-06-05	[craigsteven.com]	lockbit3	Link
2024-06-05	[Elfi-Tech]	handala	Link
2024-06-05	[Dubai Municipality (UAE)]	daixin	Link
2024-06-05	[E-T-A]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-01	[Frontier.com]	ransomhub	Link
2024-06-04	[Premium Broking House]	SenSayQ	Link
2024-06-04	[Vimer Industrie Grafiche Italiane]	SenSayQ	Link
2024-06-04	[Voorhees Family Office Services]	everest	Link
2024-06-04	[Mahindra Racing]	akira	Link
2024-06-04	[naprodgroup.com]	lockbit3	Link
2024-06-03	[Madata Data Collection & Internet Portals]	mallox	Link
2024-06-03	[Río Negro]	mallox	Link
2024-06-03	[Langescheid GbR]	arcusmedia	Link
2024-06-03	[Franja IT Integradores de Tecnología]	arcusmedia	Link
2024-06-03	[Duque Saldarriaga]	arcusmedia	Link
2024-06-03	[BHMAC]	arcusmedia	Link
2024-06-03	[Botselo]	arcusmedia	Link
2024-06-03	[Immediate Transport – UK]	arcusmedia	Link
2024-06-01	[cfymca.org]	lockbit3	Link
2024-06-03	[Northern Minerals Limited]	bianlian	Link
2024-06-03	[ISETO CORPORATION]	8base	Link
2024-06-03	[Nidec Motor Corporation]	8base	Link
2024-06-03	[Anderson Mikos Architects]	akira	Link
2024-06-03	[My City application]	handala	Link
2024-06-02	[www.eastshoresound.com]	ransomhub	Link
2024-06-02	[smithandcaugheys.co.nz]	lockbit3	Link
2024-06-01	[Frontier]	ransomhub	Link
2024-06-16	[garrettmotion.com]	dispossessor	Link
2024-06-28	[notablefrontier.com]	dispossessor	Link
2024-06-12	[energytransfer.com]	dispossessor	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.