Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240618

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

CISA warnt: Angriffe auf kritische Lücke in Progress Telerik Report Server

In der Berichtsverwaltung Progress Telerik Report Server greifen Kriminelle eine Sicherheitslücke an. Sie erlaubt die Umgehung der Authentifizierung.

- Link

—

Nextcloud: Angreifer können Zwei-Faktor-Authentifizierung umgehen

Die Clouddienst-Software Nextcloud ist verwundbar. In aktuellen Versionen haben die Entwickler mehrere Sicherheitslücken geschlossen.

- Link

—

Ivanti Endpoint Manager: Exploit für kritische Lücke aufgetaucht

Ein Proof-of-Concept-Exploit für eine kritische Lücke in Ivanti Endpoint Manager ist aufgetaucht. Zudem gibt es ein Update für den Hotfix.

- Link

—

Sicherheitsupdates: Angreifer können Asus-Router kompromittieren

Mehrere WLAN-Router von Asus sind verwundbar und Angreifer können auf sie zugreifen. Updates lösen mehrere Sicherheitsprobleme.

- Link

—

BIOS-Lücken: Angreifer können Dell-PCs kompromittieren

Unter anderem PCs der Serie Alienware und Inspiron sind vor Attacken gefährdet. Dabei kann Schadcode auf Computer gelangen.

- Link

—

CISA warnt: Kritischer PHP-Bug wird von Ransomware ausgenutzt

Automatisierte Attacken gegen Windows-Systeme mit PHP-CGI führen zur Infektion. Die Angreifer laden Schadcode nach und verschlüsseln den Server.

- Link

—

Sicherheitsupdates: Fortinet rüstet Produkte gegen verschiedene Attacken

Angreifer können Fortinet-Produkte unter anderem mit Schadcode attackieren, um Systeme zu kompromittieren. Patches stehen zum Download.

- Link

—

Angreifer attackieren Geräte: Extra-Sicherheitsupdates für Google Pixel

Patches schließen mehrere kritische Sicherheitslücken in Googles Pixel-Serie. Eine Schwachstelle soll bereits ausgenutzt werden.

- Link

—

Sicherheitsupdate: VLC media player für Attacken anfällig

Die Entwickler haben eine Sicherheitslücke im VLC media player geschlossen. Durch die Schwachstelle kann Schadcode schlüpfen.

- Link

—

Jetzt patchen! Veeam Backup Enterprise Manager vor Attacken gefährdet

Weil mittlerweile Exploitcode für eine kritische Lücke in Veeam Backup Enterprise Manager in Umlauf ist, können Attacken bevorstehen.

- 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	0.958120000	0.994510000	Link
CVE-2023-6553	0.918870000	0.989340000	Link
CVE-2023-5360	0.911260000	0.988750000	Link
CVE-2023-4966	0.969240000	0.997250000	Link
CVE-2023-48795	0.961680000	0.995200000	Link
CVE-2023-47246	0.935450000	0.991070000	Link
CVE-2023-46805	0.955460000	0.994060000	Link
CVE-2023-46747	0.972480000	0.998480000	Link
CVE-2023-46604	0.931360000	0.990680000	Link
CVE-2023-4542	0.924200000	0.989890000	Link
CVE-2023-43208	0.959780000	0.994810000	Link
CVE-2023-43177	0.960230000	0.994900000	Link
CVE-2023-42793	0.970430000	0.997620000	Link
CVE-2023-41265	0.920320000	0.989450000	Link
CVE-2023-39143	0.948440000	0.992890000	Link
CVE-2023-38646	0.900980000	0.988020000	Link
CVE-2023-38205	0.945440000	0.992400000	Link
CVE-2023-38203	0.968530000	0.997070000	Link
CVE-2023-38146	0.905210000	0.988310000	Link
CVE-2023-38035	0.974870000	0.999740000	Link
CVE-2023-36845	0.966580000	0.996440000	Link
CVE-2023-3519	0.909250000	0.988570000	Link
CVE-2023-35082	0.967870000	0.996870000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.967810000	0.996850000	Link
CVE-2023-34993	0.971450000	0.998050000	Link
CVE-2023-34960	0.922740000	0.989660000	Link
CVE-2023-34634	0.923550000	0.989750000	Link
CVE-2023-34468	0.900570000	0.988000000	Link
CVE-2023-34362	0.957100000	0.994350000	Link
CVE-2023-34039	0.944630000	0.992260000	Link
CVE-2023-3368	0.931130000	0.990640000	Link
CVE-2023-33246	0.972320000	0.998440000	Link
CVE-2023-32315	0.973460000	0.998960000	Link
CVE-2023-32235	0.902790000	0.988160000	Link
CVE-2023-30625	0.950680000	0.993250000	Link
CVE-2023-30013	0.963050000	0.995510000	Link
CVE-2023-29300	0.969840000	0.997440000	Link
CVE-2023-29298	0.943950000	0.992110000	Link
CVE-2023-28771	0.918640000	0.989330000	Link
CVE-2023-28121	0.932700000	0.990830000	Link
CVE-2023-27524	0.970620000	0.997680000	Link
CVE-2023-27372	0.973630000	0.999030000	Link
CVE-2023-27350	0.971140000	0.997910000	Link
CVE-2023-26469	0.932230000	0.990790000	Link
CVE-2023-26360	0.952190000	0.993500000	Link
CVE-2023-26035	0.965720000	0.996230000	Link
CVE-2023-25717	0.956860000	0.994300000	Link
CVE-2023-25194	0.967930000	0.996910000	Link
CVE-2023-2479	0.963760000	0.995700000	Link
CVE-2023-24489	0.973550000	0.999000000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.944080000	0.992140000	Link
CVE-2023-23397	0.922480000	0.989630000	Link
CVE-2023-23333	0.963260000	0.995570000	Link
CVE-2023-22527	0.972960000	0.998670000	Link
CVE-2023-22518	0.961970000	0.995250000	Link
CVE-2023-22515	0.973330000	0.998880000	Link
CVE-2023-21839	0.955020000	0.993980000	Link
CVE-2023-21554	0.955760000	0.994100000	Link
CVE-2023-20887	0.966680000	0.996470000	Link
CVE-2023-20198	0.915340000	0.989070000	Link
CVE-2023-1671	0.968760000	0.997120000	Link
CVE-2023-0669	0.968870000	0.997150000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 17 Jun 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Mon, 17 Jun 2024

[NEU] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] Ivanti Endpoint Manager: Mehrere Schwachstellen ermöglichen Codeausführung

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Ivanti Endpoint Manager ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 17 Jun 2024

[NEU] [hoch] Nextcloud: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Nextcloud ausnutzen, um Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, die Rechte zu erweitern und Dateien zu manipulieren.

- Link

—

Mon, 17 Jun 2024

[NEU] [hoch] FreeRADIUS: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FreeRADIUS ausnutzen, um Informationen offenzulegen.

- Link

—

Mon, 17 Jun 2024

[NEU] [hoch] wget: Schwachstelle ermöglicht nicht spezifizierten Angriff

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

- Link

—

Mon, 17 Jun 2024

[NEU] [hoch] libarchive: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libarchive ausnutzen, um beliebigen

Programmcode auszuführen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.

- Link

—

Mon, 17 Jun 2024

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

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

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] QEMU: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in QEMU ausnutzen, um seine Privilegien zu erhöhen, Code auszuführen oder einen Denial of Service zu verursachen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

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

- Link

—

Mon, 17 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

—

Mon, 17 Jun 2024

[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen SMTP Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

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

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen ermöglichen Denial of Service

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 17 Jun 2024

[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um beliebigen Code auszuführen oder einen ‘Denial of Service’-Zustand zu verursachen.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/16/2024	[Fedora 40 : thunderbird (2024-748bedc96c)]	critical
6/15/2024	[Debian dsa-5711 : thunderbird - security update]	critical
6/14/2024	[Debian dla-3827 : libcolorcorrect5 - security update]	critical
6/14/2024	[Rocky Linux 8 : webkit2gtk3 (RLSA-2024:2982)]	critical
6/17/2024	[RHEL 7 : linux-firmware (RHSA-2024:3939)]	high
6/17/2024	[Ivanti Endpoint Manager < 2022 (CVE-2024-22058)]	high
6/17/2024	[Oracle Linux 7 : firefox (ELSA-2024-3951)]	high
6/17/2024	[RHEL 8 : firefox (RHSA-2024:3952)]	high
6/17/2024	[RHEL 8 : flatpak (RHSA-2024:3962)]	high
6/17/2024	[RHEL 7 : firefox (RHSA-2024:3951)]	high
6/17/2024	[RHEL 8 : firefox (RHSA-2024:3954)]	high
6/17/2024	[RHEL 8 : flatpak (RHSA-2024:3961)]	high
6/17/2024	[RHEL 8 : firefox (RHSA-2024:3953)]	high
6/17/2024	[RHEL 8 : flatpak (RHSA-2024:3963)]	high
6/17/2024	[RHEL 8 : firefox (RHSA-2024:3950)]	high
6/17/2024	[RHEL 9 : firefox (RHSA-2024:3955)]	high
6/17/2024	[RHEL 9 : flatpak (RHSA-2024:3959)]	high
6/17/2024	[RHEL 9 : flatpak (RHSA-2024:3960)]	high
6/17/2024	[RHEL 9 : firefox (RHSA-2024:3958)]	high
6/17/2024	[RHEL 9 : firefox (RHSA-2024:3949)]	high
6/17/2024	[Ubuntu 23.10 / 24.04 LTS : Rack vulnerabilities (USN-6837-1)]	high
6/17/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : SSSD vulnerability (USN-6836-1)]	high
6/16/2024	[Debian dsa-5712 : ffmpeg - security update]	high
6/16/2024	[Debian dla-3830 : libvpx-dev - security update]	high

Datum	Schwachstelle	Bewertung
6/16/2024	[Debian dsa-5713 : libndp-dbg - security update]	high
6/15/2024	[Debian dla-3828 : atril - security update]	high
6/15/2024	[SUSE SLES15 Security Update : libaom (SUSE-SU-2024:2030-1)]	high
6/15/2024	[SUSE SLES15 / openSUSE 15 Security Update : podman (SUSE-SU-2024:2031-1)]	high
6/14/2024	[Rocky Linux 8 : container-tools:rhel8 (RLSA-2024:3254)]	high
6/14/2024	[Rocky Linux 8 : firefox (RLSA-2024:3783)]	high
6/14/2024	[Debian dsa-5710 : chromium - security update]	high
6/14/2024	[Rocky Linux 8 : python39:3.9 and python39-devel:3.9 (RLSA-2024:2985)]	high
6/14/2024	[Rocky Linux 8 : libxml2 (RLSA-2024:3626)]	high
6/14/2024	[Rocky Linux 8 : gstreamer1-plugins-bad-free (RLSA-2024:3060)]	high
6/14/2024	[Rocky Linux 8 : pki-core:10.6 and pki-deps:10.6 (RLSA-2024:3061)]	high
6/14/2024	[Ubuntu 22.04 LTS : Linux kernel (NVIDIA) vulnerabilities (USN-6818-3)]	high
6/14/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-6817-3)]	high
6/14/2024	[Ubuntu 22.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6821-4)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 17 Jun 2024

SPA-CART CMS 1.9.0.6 Username Enumeration / Business Logic Flaw

SPA-CART CMS version 1.9.0.6 suffers from business logic and user enumeration flaws.

- Link

—

” “Mon, 17 Jun 2024

Payroll Management System 1.0 Remote Code Execution

Payroll Management System version 1.0 suffers from a remote code execution vulnerability.

- Link

—

” “Mon, 17 Jun 2024

WordPress RFC WordPress 6.0.8 Shell Upload

WordPress RFC WordPress plugin version 6.0.8 suffers from a remote shell upload vulnerability.

- Link

—

” “Fri, 14 Jun 2024

Premium Support Tickets For WHMCS 1.2.10 Cross Site Scripting

Premium Support Tickets For WHMCS version 1.2.10 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 14 Jun 2024

AEGON LIFE 1.0 Cross Site Scripting

AEGON LIFE version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Fri, 14 Jun 2024

AEGON LIFE 1.0 Remote Code Execution

AEGON LIFE version 1.0 suffers from an unauthenticated remote code execution vulnerability.

- Link

—

” “Fri, 14 Jun 2024

AEGON LIFE 1.0 SQL Injection

AEGON LIFE version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Fri, 14 Jun 2024

PHP Remote Code Execution

PHP versions prior to 8.3.8 suffer from a remote code execution vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Telerik Report Server Authentication Bypass / Remote Code Execution

This Metasploit module chains an authentication bypass vulnerability with a deserialization vulnerability to obtain remote code execution against Telerik Report Server versions 10.0.24.130 and below. The authentication bypass flaw allows an unauthenticated user to create a new user with administrative privileges. The USERNAME datastore option can be used to authenticate with an existing account to prevent the creation of a new one. The deserialization flaw works by uploading a specially crafted report that when loaded will execute an OS command as NT AUTHORITY\SYSTEM. The module will automatically delete the created report but not the account because users are unable to delete themselves.

- Link

—

” “Thu, 13 Jun 2024

Rejetto HTTP File Server (HFS) Unauthenticated Remote Code Execution

The Rejetto HTTP File Server (HFS) version 2.x is vulnerable to an unauthenticated server side template injection (SSTI) vulnerability. A remote unauthenticated attacker can execute code with the privileges of the user account running the HFS.exe server process. This exploit has been tested to work against version 2.4.0 RC7 and 2.3m. The Rejetto HTTP File Server (HFS) version 2.x is no longer supported by the maintainers and no patch is available. Users are recommended to upgrade to newer supported versions.

- Link

—

” “Thu, 13 Jun 2024

Cacti Import Packages Remote Code Execution

This exploit module leverages an arbitrary file write vulnerability in Cacti versions prior to 1.2.27 to achieve remote code execution. It abuses the Import Packages feature to upload a specially crafted package that embeds a PHP file. Cacti will extract this file to an accessible location. The module finally triggers the payload to execute arbitrary PHP code in the context of the user running the web server. Authentication is needed and the account must have access to the Import Packages feature. This is granted by setting the Import Templates permission in the Template Editor section.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 Cross Site Scripting

Lost and Found Information System version 1.0 suffers from a reflective cross site scripting vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 SQL Injection

Lost and Found Information System version 1.0 suffers from an unauthenticated blind boolean-based remote SQL injection vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 SQL Injection

Lost and Found Information System version 1.0 suffers from an unauthenticated blind time-based remote SQL injection vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Lost And Found Information System 1.0 Cross Site Scripting

Lost and Found Information System version 1.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 13 Jun 2024

Quick Cart 6.7 Shell Upload

Quick Cart version 6.7 suffers from a remote shell upload vulnerability provided you have administrative privileges.

- Link

—

” “Thu, 13 Jun 2024

Quick CMS 6.7 Shell Upload

Quick CMS version 6.7 suffers from a remote shell upload vulnerability provided you have administrative privileges.

- Link

—

” “Wed, 12 Jun 2024

Carbon Forum 5.9.0 Cross Site Scripting

Carbon Forum version 5.9.0 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Wed, 12 Jun 2024

XMB 1.9.12.06 Cross Site Scripting

XMB version 1.9.12.06 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “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

—

”

4.2 0-Days der letzten 5 Tage

“Fri, 14 Jun 2024

ZDI-24-778: Linux Kernel USB Core Out-Of-Bounds Read Local Privilege Escalation Vulnerability

- Link

—

” “Fri, 14 Jun 2024

ZDI-24-777: Linux Kernel ksmbd Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Fri, 14 Jun 2024

ZDI-24-776: (Pwn2Own) Oracle VirtualBox OHCI USB Controller Use-After-Free Local Privilege Escalation Vulnerability

- Link

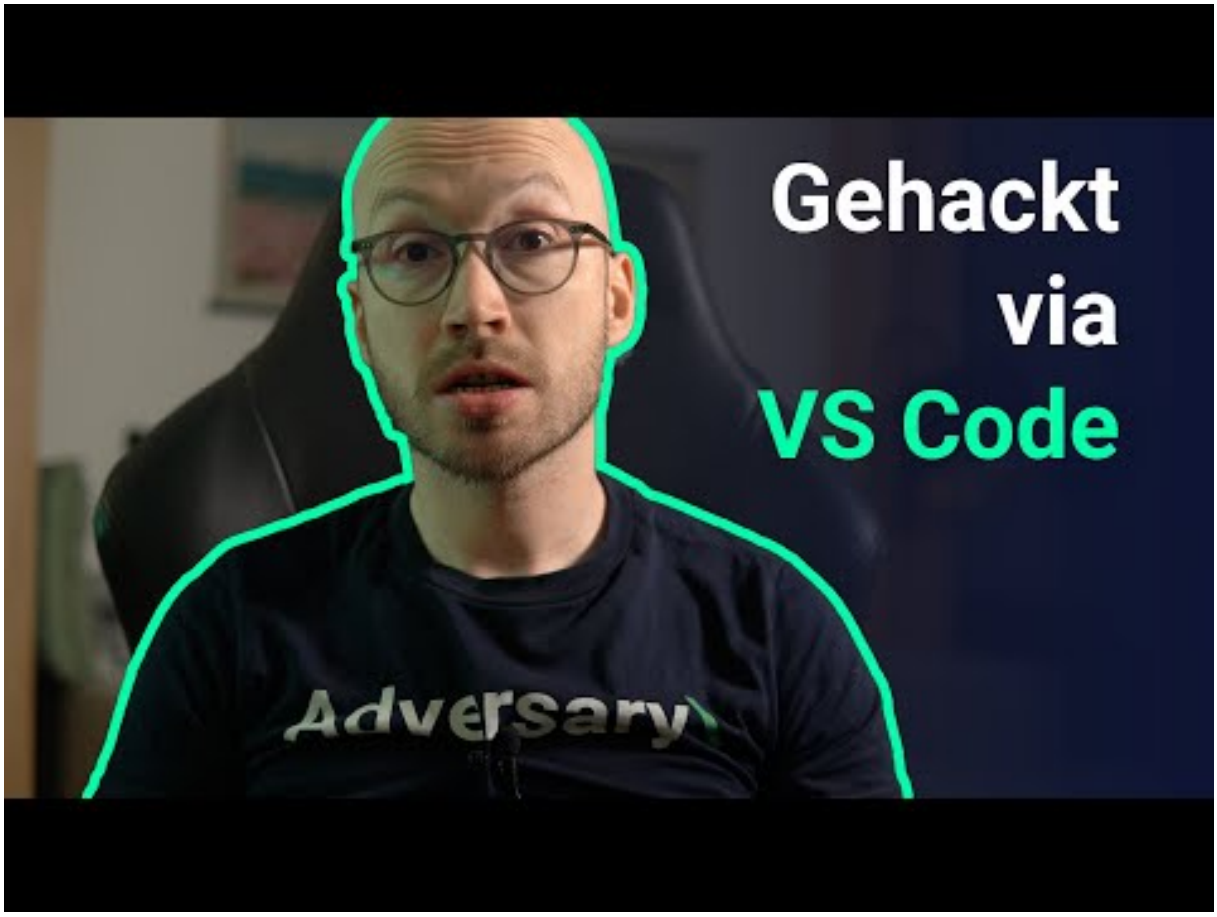
—

”

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
2024-06-17	MARINA (Maritime Industry Authority)	[PHL]	Link
2024-06-17	Rekah	[ISR]	Link
2024-06-17	Krankenhaus Agatharied	[DEU]	Link
2024-06-14	GlobalWafers	[TWN]	Link
2024-06-12	Axido	[FRA]	Link
2024-06-12	Commune de Benalmádena	[ESP]	Link
2024-06-12	Richland School District	[USA]	Link
2024-06-11	Mercatino dell'usato	[ITA]	Link
2024-06-10	Toronto District School Board (TDSB)	[CAN]	Link
2024-06-10	Crown Equipment Corporation	[USA]	Link
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
2024-06-02	Special Health Resources (SHR)	[USA]	Link

7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-10	[OCEANAIR]	incransom	Link
2024-06-17	[The Kansas City Kansas Police Department]	blacksuit	Link
2024-06-04	[northcottage.com]	qilin	Link
2024-06-17	[A-Line Staffing Solutions]	underground	Link
2024-06-13	[www.racalacoustics.com [UPDATE]]	ransomhub	Link
2024-06-17	[www.liderit.es]	ransomhub	Link
2024-06-17	[St Vincent de Paul Catholic School]	qilin	Link
2024-06-17	[Sensory Spectrum]	incransom	Link
2024-06-17	[Acteon Group]	hunters	Link
2024-06-17	[pkaufmann.com]	blackbasta	Link
2024-06-17	[modplan.co.uk]	blackbasta	Link
2024-06-17	[wielton.com.pl]	blackbasta	Link
2024-06-17	[grupoamper.com]	blackbasta	Link
2024-06-17	[TETRA Technologies, Inc.]	akira	Link
2024-06-16	[parlorenzo.com]	ransomhub	Link
2024-06-17	[www.domainatcleveland.com]	ransomhub	Link
2024-06-01	[Virum Apotek]	ransomhouse	Link
2024-06-17	[SolidCAM 2024 SP0]	handala	Link
2024-06-17	[Next Step Healthcare]	qilin	Link
2024-06-17	[cosimti.com]	darkvault	Link
2024-06-17	[fifcousa.com]	dAn0n	Link
2024-06-17	[mgfsourcing.com]	blackbasta	Link
2024-06-17	[journohq.com]	darkvault	Link
2024-06-16	[colfax.k12.wi.us]	blacksuit	Link
2024-06-16	[Production Machine & Enterprises]	rhysida	Link
2024-06-16	[CETOS Services]	rhysida	Link
2024-06-15	[Kiemle-Hankins]	rhysida	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-15	[Legrand CRM]	hunters	Link
2024-06-15	[MRI]	hunters	Link
2024-06-15	[Ma'agan Michael Kibbutz]	handala	Link
2024-06-15	[Oahu Transit Services]	dragonforce	Link
2024-06-12	[Sun City Pediatrics PA (USA, TX)]	spacebears	Link
2024-06-11	[Lee Trevino Dental (USA,TX)]	spacebears	Link
2024-06-15	[Peregrine Petroleum]	blacksuit	Link
2024-06-15	[Mountjoy]	bianlian	Link
2024-06-14	[svmasonry.com]	qilin	Link
2024-06-14	[MBE CPA]	metaencryptor	Link
2024-06-14	[EnviroApplications]	qilin	Link
2024-06-14	[www.gannons.co.uk]	apt73	Link
2024-06-14	[New Balance Commodities]	akira	Link
2024-06-14	[Victoria Racing Club]	medusa	Link
2024-06-14	[Mundocar.eu]	cloak	Link
2024-06-13	[Cukierski & Associates, LLC]	everest	Link
2024-06-13	[Diogenet S.r.l.]	everest	Link
2024-06-13	[2K Dental]	everest	Link
2024-06-13	[Dordt University]	bianlian	Link
2024-06-13	[Borrer Executive Search]	apt73	Link
2024-06-13	[www.bigalsfoodservice.co.uk]	apt73	Link
2024-06-13	[www.racalacoustics.com]	ransomhub	Link
2024-06-13	[Kito Canada]	incransom	Link
2024-06-11	[Bock & Associates, LLP]	qilin	Link
2024-06-12	[Walder Wyss and Partners]	play	Link
2024-06-12	[Celluphone]	play	Link
2024-06-12	[Me Too Shoes]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-12	[Ab Monsteras Metall]	play	Link
2024-06-12	[Amarilla Gas]	play	Link
2024-06-12	[Aldenhoven]	play	Link
2024-06-12	[ANTECH-GUTLING Gruppe]	play	Link
2024-06-12	[Refcio & Associates]	play	Link
2024-06-12	[City Builders]	play	Link
2024-06-12	[Eurotrol B.V.]	blacksuit	Link
2024-06-12	[Seagulf Marine Industries]	play	Link
2024-06-12	[Western Mechanical]	play	Link
2024-06-12	[Trisun Land Services]	play	Link
2024-06-10	[GEMCO Constructors]	medusa	Link
2024-06-10	[Dynamo Electric]	medusa	Link
2024-06-11	[Farnell Packaging]	medusa	Link
2024-06-12	[hydefuel.com]	qilin	Link
2024-06-12	[Diverse Technology Industrial]	play	Link
2024-06-12	[Air Cleaning Specialists]	play	Link
2024-06-12	[Corbin Turf & Ornamental Supply]	play	Link
2024-06-12	[Kinter]	play	Link
2024-06-12	[Goodman Reichwald-Dodge]	play	Link
2024-06-12	[3GL Technology Solutions]	play	Link
2024-06-12	[Brainworks Software]	play	Link
2024-06-12	[Eagle Materials]	play	Link
2024-06-12	[Great Lakes International Trading]	play	Link
2024-06-12	[Smartweb]	play	Link
2024-06-12	[Peterbilt of Atlanta]	play	Link
2024-06-12	[Chroma Color]	play	Link
2024-06-12	[Shinnick & Ryan]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-12	[ZeepLive]	darkvault	Link
2024-06-12	[Concrete]	hunters	Link
2024-06-12	[IPM Group (Multimedia Information & Production Company)]	akira	Link
2024-06-12	[manncorp.com]	lockbit3	Link
2024-06-12	[sgvfr.com]	trinity	Link
2024-06-12	[CBSTRAINING]	trinity	Link
2024-06-11	[Kutes.com]	redransomware	Link
2024-06-11	[www.novabitsrl.it]	ransomhub	Link
2024-06-11	[smicusa.com]	ransomhub	Link
2024-06-11	[www.ham.org.br]	ransomhub	Link
2024-06-12	[NJORALSURGERY.COM]	clop	Link
2024-06-11	[SolidCAM LEAK]	handala	Link
2024-06-12	[Zuber Gardner CPAs pt.2]	everest	Link
2024-06-09	[Seafrigo]	dragonforce	Link
2024-06-12	[Special Health Resources]	blacksuit	Link
2024-06-11	[WinFashion ERP]	arcusmedia	Link
2024-06-12	[apex.uk.net]	apt73	Link
2024-06-12	[AlphaNovaCapital]	apt73	Link
2024-06-12	[AMI Global Assistance]	apt73	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-10	[transportlaberge.com]	cactus	Link
2024-06-10	[sanyo-shokai.co.jp]	cactus	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-06	[ssiworld.com]	blackbasta	Link
2024-06-06	[driver-group.com]	blackbasta	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-06-05	[Dubai Municipality (UAE)]	daixin	Link
2024-06-05	[E-T-A]	akira	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.