Cybersecurity Morgenreport

Ausgabe: 20231109

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

Security-News

Heise - Security-Alert

Malware-Schutz: Rechteausweitung in Trend Micros Apex One möglich
In Trend Micros Schutzsoftware Apex One können Angreifer Schwachstellen missbrauchen, um ihre Privilegien auszuweiten. Updates korrigieren das.
- Link

—

Patchday: Kritische System-Lücke bedroht Android 11, 12 und 13
Google hat wichtige Sicherheitsupdates für verschiedene Android-Versionen veröffentlicht.
- Link

—

Webbrowser: Google Chrome-Update dichtet Lücke mit hohem Risiko ab
Google schließt mit dem Update von Chrome eine hochriskante Sicherheitslücke, die Webseiten offenbar das Unterschieben von Schadcode ermöglicht.
- Link

—

Kritische Atlassian-Confluence-Lücke wird angegriffen
Vergangene Woche hat Atlassian eine Sicherheitslücke in Confluence geschlossen. Kriminelle missbrauchen sie inzwischen.
- Link

—

Sicherheitsupdates: Zwei kritische Lücken bedrohen Monitoringtool Veeam One
Die Entwickler haben in Veeam One unter anderem zwei kritische Schwachstellen geschlossen. Im schlimmsten Fall kann Schadcode auf Systeme gelangen.
- Link

—

Sicherheitsupdates QNAP: Angreifer können eigene Befehle auf NAS ausführen
Wichtige Sicherheitspatches sichern Netzwerkspeicher von QNAP ab. Unbefugte können Daten einsehen.
- Link

—

Microsoft Exchange Server anfällig für Remotecode-Ausführung und Datenklau
Vier Schwachstellen im Exchange-Server machen die Groupware anfällig für Cyberangriffe. Drei Lücken werden bald geschlossen, eine ist bereits abgedichtet.
- Link

—

Sicherheitsupdates Nvidia: GeForce-Treiberlücken gefährden PCs
Nvidias Entwickler haben im Grafikkartentreiber und der VGPU-Software mehrere Sicherheitslücken geschlossen.
- Link

—

Solarwinds Platform 2023.4 schließt Codeschmuggel-Lücken
Solarwinds hat das Platform-Update auf Version 2023.4 veröffentlicht. Neben diversen Fehlerkorrekturen schließt es auch Sicherheitslücken.
- Link

—

Sicherheitslücken: Angreifer können Cisco-Firewalls manipulieren
Mehrere Schwachstellen gefährden unter anderem Cisco Firepower und Identity Services Engine. Patches sind verfügbar.
- Link

—

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.

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.

CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-4966	0.922670000	0.986960000	Link
CVE-2023-46747	0.969840000	0.996640000	Link
CVE-2023-42793	0.972640000	0.998090000	Link
CVE-2023-38035	0.970400000	0.996880000	Link
CVE-2023-35078	0.963850000	0.994270000	Link
CVE-2023-34362	0.921790000	0.986840000	Link
CVE-2023-33246	0.970860000	0.997120000	Link
CVE-2023-32315	0.957520000	0.992590000	Link
CVE-2023-30625	0.938840000	0.989130000	Link
CVE-2023-30013	0.936180000	0.988710000	Link
CVE-2023-28771	0.918550000	0.986470000	Link
CVE-2023-27372	0.970490000	0.996910000	Link
CVE-2023-27350	0.971560000	0.997500000	Link
CVE-2023-26469	0.918080000	0.986400000	Link
CVE-2023-26360	0.913940000	0.985980000	Link
CVE-2023-25717	0.962680000	0.993850000	Link
CVE-2023-25194	0.910980000	0.985680000	Link
CVE-2023-2479	0.961630000	0.993520000	Link
CVE-2023-24489	0.969080000	0.996340000	Link
CVE-2023-22515	0.955290000	0.992070000	Link
CVE-2023-21839	0.960250000	0.993180000	Link
CVE-2023-21823	0.951390000	0.991270000	Link
CVE-2023-21554	0.961220000	0.993420000	Link
CVE-2023-20887	0.945440000	0.990280000	Link
CVE-2023-20198	0.916150000	0.986220000	Link
CVE-2023-0669	0.965820000	0.995000000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 08 Nov 2023

[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Developer Tools ausnutzen, um seine Privilegien zu erhöhen und einen Denial of Service Zustand zu verursachen.

- Link

—

Wed, 08 Nov 2023
[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Wed, 08 Nov 2023
[UPDATE] [hoch] Red Hat Satellite: Mehrere Schwachstellen
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Wed, 08 Nov 2023
[UPDATE] [hoch] Squid: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link
—
Wed, 08 Nov 2023
[NEU] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen
Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.
- Link
—
Wed, 08 Nov 2023
[NEU] [hoch] Progress Software WS_FTP: Schwachstelle ermöglicht Manipulation von Dateien
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Progress Software WS_FTP ausnutzen, um Dateien zu manipulieren.
- Link
—
Wed, 08 Nov 2023
[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.
- Link
—
Wed, 08 Nov 2023
[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
—
Wed, 08 Nov 2023
[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.
- Link
—
Wed, 08 Nov 2023
[UPDATE] [hoch] Python: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Wed, 08 Nov 2023
[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

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Grafana ausnutzen, um Benutzerrechte zu erlangen, seine Privilegien zu erweitern und um Informationen offenzulegen.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Grafana ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, Informationen falsch darzustellen und seine Privilegien zu erweitern.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff und einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] X.Org X11: Schwachstelle ermöglicht Privilegieneskalation oder Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in X.Org X11 ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Linux Kernel (vmwgfx): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

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

- Link

—

Wed, 08 Nov 2023

[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/8/2023	[Atlassian Confluence Authentication Bypass (CONFSERVER-93142) (Direct Check)]	critical
11/8/2023	[Fedora 37 : salt (2023-89e8f3efc5)]	critical
11/8/2023	[Google Chrome < 119.0.6045.123 Vulnerability]	critical
11/8/2023	[Google Chrome < 119.0.6045.123 Vulnerability]	critical
11/8/2023	[RHEL 8 : squid:4 (RHSA-2023:6803)]	critical
11/8/2023	[RHEL 8 : squid:4 (RHSA-2023:6801)]	critical
11/8/2023	[RHEL 8 : squid:4 (RHSA-2023:6810)]	critical
11/8/2023	[RHEL 7 : squid (RHSA-2023:6805)]	critical
11/8/2023	[RHEL 8 : fence-agents bug fix, enhancement, and (RHSA-2023:6812)]	critical
11/8/2023	[RHEL 8 : squid:4 (RHSA-2023:6804)]	critical
11/8/2023	[Fedora 38 : salt (2023-a6699df922)]	critical
11/8/2023	[Oracle Linux 8 : squid:4 (ELSA-2023-6267)]	critical
11/8/2023	[FreeBSD : chromium – security update (77fc311d-7e62-11ee-8290-a8a1599412c6)]	critical
11/8/2023	[Fedora 39 : salt (2023-3eda7b85f5)]	critical
11/8/2023	[NewStart CGSL MAIN 6.06 : libksba Vulnerability (NS-SA-2023-0140)]	critical
11/8/2023	[Slackware Linux 14.0 / 14.1 / 14.2 / 15.0 / current sudo Multiple Vulnerabilities (SSA:2023-311-01)]	high
11/8/2023	[Fedora 38 : mlpack (2023-23c0bd9a45)]	high
11/8/2023	[Fedora 39 : mlpack (2023-862bb40df5)]	high
11/8/2023	[Fedora 37 : chromium (2023-14b8d5c44f)]	high
11/8/2023	[Fedora 37 : open-vm-tools (2023-1ed0ec0035)]	high
11/8/2023	[Fedora 39 : open-vm-tools (2023-86a50ffc72)]	high
11/8/2023	[RHEL 8 : kernel (RHSA-2023:6813)]	high
11/8/2023	[RHEL 7 : insights-client (RHSA-2023:6795)]	high
11/8/2023	[RHEL 8 : tigervnc (RHSA-2023:6808)]	high
11/8/2023	[FreeBSD : FreeBSD – libc stdio buffer overflow (5afcc9a4-7e04-11ee-8e38-002590c1f29c)]	high
11/8/2023	[Debian DLA-3647-1 : trapperkeeper-webserver-jetty9-clojure - LTS security update]	high
11/8/2023	[RHEL 7 : rh-python38-python (RHSA-2023:6793)]	high
11/8/2023	[RHEL 8 : insights-client (RHSA-2023:6811)]	high
11/8/2023	[RHEL 8 : insights-client (RHSA-2023:6798)]	high
11/8/2023	[Fedora 37 : mlpack (2023-dde357b985)]	high
11/8/2023	[Fedora 38 : open-vm-tools (2023-08e2bb6815)]	high
11/8/2023	[RHEL 7 : xorg-x11-server (RHSA-2023:6802)]	high
11/8/2023	[RHEL 9 : insights-client (RHSA-2023:6796)]	high
11/8/2023	[Debian DLA-3649-1 : python-urllib3 - LTS security update]	high
11/8/2023	[RHEL 8 : mariadb:10.5 (RHSA-2023:6821)]	high
11/8/2023	[RHEL 8 : mariadb:10.5 (RHSA-2023:6822)]	high
11/8/2023	[NewStart CGSL MAIN 6.06 : libxml2 Multiple Vulnerabilities (NS-SA-2023-0131)]	high
11/8/2023	[NewStart CGSL MAIN 6.06 : c-ares Vulnerability (NS-SA-2023-0136)]	high
11/8/2023	[NewStart CGSL MAIN 6.06 : qemu Multiple Vulnerabilities (NS-SA-2023-0132)]	high
11/7/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : urllib3 vulnerabilities (USN-6473-1)]	high
11/7/2023	[Mitsubishi Electric GOT and Tension Controller (CVE-2021-20589)]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“Fri, 27 Oct 2023
Splunk edit_user Capability Privilege Escalation
Splunk suffers from an issue where a low-privileged user who holds a role that has the edit_user capability assigned to it can escalate their privileges to that of the admin user by providing a specially crafted web request. This is because the edit_user capability does not honor the grantableRoles setting in the authorize.conf configuration file, which prevents this scenario from happening. This exploit abuses this vulnerability to change the admin password and login with it to upload a malicious app achieving remote code execution.
- Link
—
” “Fri, 27 Oct 2023
phpFox 4.8.13 PHP Object Injection
phpFox versions 4.8.13 and below have an issue where user input passed through the ”url” request parameter to the /core/redirect route is not properly sanitized before being used in a call to the unserialize() PHP function. This can be exploited by remote, unauthenticated attackers to inject arbitrary PHP objects into the application scope, allowing them to perform a variety of attacks, such as executing arbitrary PHP code.
- Link
—
” “Fri, 27 Oct 2023
SugarCRM 13.0.1 Shell Upload
SugarCRM versions 13.0.1 and below suffer from a remote shell upload vulnerability in the set_note_attachment SOAP call.
- Link
—
” “Fri, 27 Oct 2023
SugarCRM 13.0.1 Server-Side Template Injection
SugarCRM versions 13.0.1 and below suffer from a server-side template injection vulnerability in the GetControl action from the Import module. This issue can be leveraged to execute arbitrary php code.
- Link
—
” “Fri, 27 Oct 2023
XAMPP 3.3.0 Buffer Overflow
XAMPP version 3.3.0 .ini unicode + SEH buffer overflow exploit.
- Link
—
” “Thu, 26 Oct 2023
TEM Opera Plus FM Family Transmitter 35.45 Cross Site Request Forgery
TEM Opera Plus FM Family Transmitter version 35.45 suffers from a cross site request forgery vulnerability.
- Link
—
” “Thu, 26 Oct 2023
TEM Opera Plus FM Family Transmitter 35.45 Remote Code Execution
TEM Opera Plus FM Family Transmitter version 35.45 suffers from a remote code execution vulnerability.
- Link
—
” “Thu, 26 Oct 2023
WordPress AI ChatBot 4.8.9 SQL Injection / Traversal / File Deletion
WordPress AI ChatBot plugin versions 4.8.9 and below suffer from arbitrary file deletion, remote SQL injection, and directory traversal vulnerabilities.
- Link
—
” “Thu, 26 Oct 2023
Oracle 19c / 21c Sharding Component Password Hash Exposure
Oracle database versions 19.3 through 19.20 and 21.3 through 21.11 have an issue where an account with create session and select any dictionary can view password hashes stored in a system table that is part of a sharding component setup.
- Link
—

” “Wed, 25 Oct 2023

Citrix Bleed Session Token Leakage Proof Of Concept

Citrix NetScaler ADC and NetScaler Gateway proof of concept exploit for the session token leakage vulnerability as described in CVE-2023-4966.

- Link

—

” “Tue, 24 Oct 2023

WordPress LiteSpeed Cache 5.6 Cross Site Scripting

WordPress LiteSpeed Cache plugin versions 5.6 and below suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 24 Oct 2023

VMWare Aria Operations For Networks SSH Private Key Exposure

VMWare Aria Operations for Networks (vRealize Network Insight) versions 6.0.0 through 6.10.0 do not randomize the SSH keys on virtual machine initialization. Since the key is easily retrievable, an attacker can use it to gain unauthorized remote access as the ”support” (root) user.

- Link

—

” “Mon, 23 Oct 2023

Moodle 4.3 Cross Site Scripting

Moodle version 4.3 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 23 Oct 2023

PowerVR Out-Of-Bounds Access / Information Leak

PowerVR suffers from a multitude of memory management bugs including out-of-bounds access and information leakage.

- Link

—

” “Fri, 20 Oct 2023

VIMESA VHF/FM Transmitter Blue Plus 9.7.1 Denial Of Service

VIMESA VHF/FM Transmitter Blue Plus version 9.7.1 suffers from a denial of service vulnerability. An unauthenticated attacker can issue an unauthorized HTTP GET request to the unprotected endpoint doreboot and restart the transmitter operations.

- Link

—

” “Thu, 19 Oct 2023

Atlassian Confluence Unauthenticated Remote Code Execution

This Metasploit module exploits an improper input validation issue in Atlassian Confluence, allowing arbitrary HTTP parameters to be translated into getter/setter sequences via the XWorks2 middleware and in turn allows for Java objects to be modified at run time. The exploit will create a new administrator user and upload a malicious plugins to get arbitrary code execution. All versions of Confluence between 8.0.0 through to 8.3.2, 8.4.0 through to 8.4.2, and 8.5.0 through to 8.5.1 are affected.

- Link

—

” “Wed, 18 Oct 2023

Squid Caching Proxy Proof Of Concepts

Two and a half years ago an independent audit was performed on the Squid Caching Proxy, which ultimately resulted in 55 vulnerabilities being discovered in the project’s C++ source code. Although some of the issues have been fixed, the majority (35) remain valid. The majority have not been assigned CVEs, and no patches or workarounds are available. Some of the listed issues concern more than one bug, which is why 45 issues are listed, despite there being 55 vulnerabilities in total (10 extra of the result of similar, but different pathways to reproduce a vulnerability). After two and a half years of waiting, the researcher has decided to release the issues publicly. This archive contains all of the proof of concept code released by the researcher.

- Link

—

” “Tue, 17 Oct 2023

XNSoft Nconvert 7.136 Buffer Overflow / Denial Of Service

XNSoft Nconvert version 7.136 is vulnerable to buffer overflow and denial of service conditions. Proof of concepts included.

- Link

—

” “Mon, 16 Oct 2023

NLB mKlik Makedonija 3.3.12 SQL Injection

NLB mKlik Makedonija version 3.3.12 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 16 Oct 2023

Linux DCCP Information Leak

Linux suffers from a small remote binary information leak in DCCP.

- Link

—

” “Mon, 16 Oct 2023

Microsoft Windows Kernel Out-Of-Bounds Reads / Memory Disclosure

The Microsoft Windows Kernel suffers from out-of-bounds reads and paged pool memory disclosure in VrpUpdateKeyInformation.

- Link

—

” “Mon, 16 Oct 2023

Microsoft Windows Kernel Paged Pool Memory Disclosure

The Microsoft Windows Kernel suffers from a paged pool memory disclosure in VrpPostEnumerateKey.

- Link

—

” “Mon, 16 Oct 2023

WordPress Royal Elementor 1.3.78 Shell Upload

WordPress Royal Elementor plugin versions 1.3.78 and below suffer from a remote shell upload vulnerability.

- Link

—

” “Mon, 16 Oct 2023

WordPress WP ERP 1.12.2 SQL Injection

WordPress WP ERP plugin versions 1.12.2 and below suffer from a remote SQL injection vulnerability.

- Link

—

” “Mon, 16 Oct 2023

ChurchCRM 4.5.4 SQL Injection

ChurchCRM version 4.5.4 suffers from a remote authenticated blind SQL injection vulnerability.

- Link

—

”

0-Day

“Mon, 06 Nov 2023

ZDI-23-1590: VMware vCenter Server Appliance DCE/RPC Protocol Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Mon, 06 Nov 2023

ZDI-23-1589: VMware Workstation UHCI Uninitialized Variable Information Disclosure Vulnerability

- Link

—

” “Mon, 06 Nov 2023

ZDI-23-1588: Microsoft Azure US Accelarators Synapse SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability

- Link

—

” “Mon, 06 Nov 2023

ZDI-23-1587: Microsoft Windows win32kfull UMPDDrvCopyBits Use-After-Free Local Privilege Escalation Vulnerability

- Link

—
” “Mon, 06 Nov 2023
ZDI-23-1586: SolarWinds Network Configuration Manager SaveResultsToFile Directory Traversal Remote Code Execution Vulnerability
- Link
—
” “Mon, 06 Nov 2023
ZDI-23-1585: SolarWinds Network Configuration Manager ExportConfigs Directory Traversal Remote Code Execution Vulnerability
- Link
—
” “Mon, 06 Nov 2023
ZDI-23-1584: SolarWinds Orion Platform BlacklistedFilesChecker Incomplete List of Disallowed Inputs Remote Code Execution Vulnerability
- Link
—
” “Mon, 06 Nov 2023
ZDI-23-1583: Google Chromium Vulkan SwiftShader Double Free Remote Code Execution Vulnerability
- Link
—
” “Mon, 06 Nov 2023
ZDI-23-1582: Tenable Nessus Link Following Local Privilege Escalation Vulnerability
- Link
—
”

Die Hacks der Woche

mit Martin Haunschmid

“I don’t know how to unf*ck this” willst du nicht in deiner Anklage lesen

Zum Youtube Video

Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2023-11-07	Comhairle nan Eilean Siar	[GBR]	Link
2023-11-06	KaDeWe	[DEU]	Link
2023-11-05	Le conseil départemental du Loiret	[FRA]	Link
2023-11-05	Madison Memorial Hospital	[USA]	Link
2023-11-05	Pulaski County Public Schools (PCPS)	[USA]	Link
2023-11-02	Infosys McCamish Systems	[USA]	Link
2023-11-02	Crystal Run Healthcare	[USA]	Link
2023-11-01	Mr. Cooper Group	[USA]	Link

Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-08	[JS Hovnanian & Sons]	play	Link
2023-11-08	[Identification Products]	play	Link
2023-11-08	[M.R. Williams]	play	Link
2023-11-08	[DESIGNA Verkehrsleittechnik]	play	Link
2023-11-08	[The Supply Room Companies & Citron WorkSpaces]	play	Link
2023-11-08	[Ackerman-Estvold]	play	Link
2023-11-08	[Meindl]	play	Link
2023-11-08	[Conditioned Air]	play	Link
2023-11-08	[Inclinator]	play	Link
2023-11-08	[Crown Supply Co]	play	Link
2023-11-08	[fawry.com]	lockbit3	Link
2023-11-08	[amberhillgroup.com]	lockbit3	Link
2023-11-08	[califanocarrelli.it]	blackbasta	Link
2023-11-08	[sheehyware.com]	alphv	Link
2023-11-08	[Michael Garron Hospital]	akira	Link
2023-11-08	[foley.k12.mn.us]	lockbit3	Link
2023-11-08	[gitiusa.com]	lockbit3	Link
2023-11-08	[allenovery.com]	lockbit3	Link
2023-11-08	[NeoDomos]	ciphbit	Link
2023-11-07	[Bakrie Group & Bakrie Sumatera Plantations]	alphv	Link
2023-11-07	[Indah Water Konsortium]	rhysida	Link
2023-11-07	[Access to the large database of a US Medical organization]	everest	Link
2023-11-07	[h-tube.com]	blackbasta	Link
2023-11-07	[torrescpa.com]	blackbasta	Link
2023-11-07	[tt-engineering.nl]	blackbasta	Link
2023-11-07	[nicecloud.nl]	blackbasta	Link
2023-11-07	[triflex.nl]	blackbasta	Link
2023-11-07	[cozwolle.nl]	blackbasta	Link
2023-11-07	[Certified Mortgage Planners]	alphv	Link
2023-11-07	[BioPower SustainableEnergy Corporation]	akira	Link
2023-11-07	[BITZER]	akira	Link
2023-11-07	[acawtrustfunds.ca]	blackbasta	Link
2023-11-07	[secci.ca]	blackbasta	Link
2023-11-07	[Hopewell Area School District]	medusa	Link
2023-11-07	[panaya]	cuba	Link
2023-11-07	[prime-art]	cuba	Link
2023-11-07	[ccdrc.pt]	lockbit3	Link
2023-11-07	[Yuxin Automobile Co.Ltd]	ragroup	Link
2023-11-07	[Aceromex (Unpay-Start Leaking)]	ragroup	Link
2023-11-07	[Japan Aviation Electronics Industry, Ltd]	alphv	Link
2023-11-06	[sacksteinlaw.com]	blackbasta	Link
2023-11-06	[good-lawyer.com]	lockbit3	Link
2023-11-06	[EFU Life Assurance]	incransom	Link
2023-11-06	[kbrlaw.com]	lockbit3	Link
2023-11-06	[eyephy.com]	lockbit3	Link
2023-11-06	[Mount St. Mary's Seminary]	rhysida	Link
2023-11-06	[concretevalue.com]	lockbit3	Link
2023-11-06	[howlandlaw.net]	lockbit3	Link
2023-11-06	[GEOCOM]	cactus	Link
2023-11-06	[MultiMasters]	cactus	Link
2023-11-06	[UTI Group]	cactus	Link
2023-11-06	[Comfloresta]	alphv	Link
2023-11-05	[Currax Pharmaceuticals]	alphv	Link
2023-11-05	[Advarra leak]	alphv	Link
2023-11-05	[Weidmann & Associates]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-05	[Unimed Blumenau]	medusa	Link
2023-11-05	[Leaguers]	medusa	Link
2023-11-05	[Zon Beachside]	medusa	Link
2023-11-05	[Canadian Psychological Association]	medusa	Link
2023-11-05	[Corsica-Ferries]	alphv	Link
2023-11-05	[penanshin]	alphv	Link
2023-11-05	[lathamcenters.org]	abyss	Link
2023-11-05	[Assurius.be]	qilin	Link
2023-11-05	[unique-relations.at]	qilin	Link
2023-11-05	[SMH Group]	rhysida	Link
2023-11-05	[nckb.com]	lockbit3	Link
2023-11-05	[egco.com]	lockbit3	Link
2023-11-05	[benya.capital]	lockbit3	Link
2023-11-05	[global-value-web.com]	lockbit3	Link
2023-11-05	[aseankorea.org]	lockbit3	Link
2023-11-05	[brlogistics.net]	lockbit3	Link
2023-11-05	[bresselouhannaiseintercom.fr]	lockbit3	Link
2023-11-05	[nfcc.gov.my]	lockbit3	Link
2023-11-05	[sansasecurity.com]	lockbit3	Link
2023-11-05	[emiliacentrale.it]	lockbit3	Link
2023-11-05	[letillet.btprms.com]	lockbit3	Link
2023-11-05	[ospedalecoq.it]	lockbit3	Link
2023-11-05	[springeroil.com]	lockbit3	Link
2023-11-05	[szutest.cz]	lockbit3	Link
2023-11-05	[mat-antriebstechnik.de]	lockbit3	Link
2023-11-05	[studio483.com]	lockbit3	Link
2023-11-04	[infosysbpm.com]	lockbit3	Link
2023-11-04	[tks.co.th]	lockbit3	Link
2023-11-03	[GeoPoint Surveying]	play	Link
2023-11-03	[APERS]	ciphbit	Link
2023-11-03	[translink.se]	lockbit3	Link
2023-11-03	[tasl.co.th]	lockbit3	Link
2023-11-03	[abhmfg.com]	lockbit3	Link
2023-11-03	[Livability]	incransom	Link
2023-11-03	[portlandtractor.com]	lockbit3	Link
2023-11-03	[unimed.coop.br]	lockbit3	Link
2023-11-03	[jewell.edu]	lockbit3	Link
2023-11-03	[microtrain.net]	lockbit3	Link
2023-11-02	[Warning to Advarra & Gadi!]	alphv	Link
2023-11-01	[Bry-Air]	play	Link
2023-11-02	[JDRM Engineering]	play	Link
2023-11-02	[Craft-Maid]	play	Link
2023-11-02	[Hilyard's]	play	Link
2023-11-02	[North Dakota Grain Inspection Services]	play	Link
2023-11-02	[Gsp Components]	play	Link
2023-11-02	[Ricardo]	play	Link
2023-11-02	[bindagroup.com]	lockbit3	Link
2023-11-02	[lafase.cl]	lockbit3	Link
2023-11-02	[shimano.com]	lockbit3	Link
2023-11-02	[Contact Cottrell and McCullough]	alphv	Link
2023-11-02	[psmicorp.com]	lockbit3	Link
2023-11-02	[imancorp.es]	blackbasta	Link
2023-11-02	[AF Supply]	alphv	Link
2023-11-02	[GO! Handelsschool Aalst]	rhysida	Link
2023-11-01	[Groupe Faubourg]	8base	Link
2023-11-02	[HAL Allergy]	alphv	Link
2023-11-01	[Detroit Symphony Orchestra]	snatch	Link
2023-11-02	[degregoris.com]	lockbit3	Link
2023-11-02	[Bluewater Health (CA) and others]	daixin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-11-01	[vitaresearch.com]	lockbit3	Link
2023-11-01	[sanmiguel.iph]	lockbit3	Link
2023-11-01	[steelofcarolina.com]	lockbit3	Link
2023-11-01	[raumberg-gumpenstein.at]	lockbit3	Link
2023-11-01	[kitprofs.com]	lockbit3	Link
2023-11-01	[imprex.es]	lockbit3	Link
2023-11-01	[Hawkeye Area Community Action Program, Inc]	blacksuit	Link
2023-11-01	[Advarra Inc]	alphv	Link
2023-11-01	[summithealth.com]	lockbit3	Link
2023-11-01	[US Claims Solutions]	knight	Link
2023-11-01	[strongtie.com]	blackbasta	Link
2023-11-01	[ampersand.tv]	blackbasta	Link
2023-11-01	[baccarat.com]	blackbasta	Link
2023-11-01	[piemmeonline.it]	blackbasta	Link
2023-11-01	[fortive.com]	blackbasta	Link
2023-11-01	[gannons.co.uk]	blackbasta	Link
2023-11-01	[gsp.com.br]	blackbasta	Link
2023-11-01	[TANATEX Chemicals]	metaencryptor	Link
2023-11-01	[edwardian.com]	blackbasta	Link
2023-11-01	[bionpharma.com]	blackbasta	Link
2023-11-01	[stantonwilliams.com]	blackbasta	Link
2023-11-01	[hugohaeffner.com]	blackbasta	Link
2023-11-01	[intred.it]	blackbasta	Link
2023-11-01	[Town of Lowa]	alphv	Link
2023-11-01	[Traxall France]	8base	Link
2023-11-01	[Armstrong Consultants]	8base	Link
2023-11-01	[JAI A/S]	8base	Link
2023-11-01	[Schöler Fördertechnik AG]	8base	Link

Quellen

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

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.