Cybersecurity Morgenreport

Ausgabe: 20231103

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

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

—

CitrixBleed: Ransomware-Banden attackieren Citrix NetScaler
Derzeit schlüpfen Erpressungstrojaner durch eine kritische Sicherheitslücke in Citrix Netscaler ADC und Gateway. Sicherheitspatches stehen bereit.
- Link

—

Jetzt patchen! Attacken auf BIG-IP-Appliances beobachtet
F5 warnt vor Angriffen auf BIG-IP-Appliances. Sicherheitspatches stehen bereit. Eine Lücke gilt als kritisch.
- Link

—

Webbrowser: Google Chrome bessert 15 Schwachstellen aus und kann HTTPS-Upgrades
Google hat den Webbrowser Chrome in Version 119 veröffentlicht. Sie schließt 15 Sicherheitslücken und etabliert den HTTPS-Upgrade-Mechanismus.
- Link

—

Jetzt patchen: Kritische Sicherheitslücke in Confluence aufgetaucht
In Confluence Server und Data Center klafft ein gefährlicher Bug – Atlassian drängt Administratoren zu zügigen Updates. Details sind Mangelware.
- Link

—

Sicherheitslücken: Angreifer können Schadcode in SugarCRM hochladen
Die Managementlösung für Kundendaten SugarCRM ist verwundbar. Gegen mögliche Attacken gerüstete Versionen schaffen Abhilfe.
- Link

—

Konfigurationsprogramm von BIG-IP-Appliances als Sprungbrett für Angreifer
F5 hat wichtige Sicherheitsupdates für BIG-IP-Produkte veröffentlicht. Angreifer können Geräte kompromittieren.
- Link

—

Lücken in Nessus Network Monitor ermöglichen Rechteerhöhung
Eine neue Version vom Nessus Network Monitor schließt Sicherheitslücken, durch die Angreifer etwa ihre Rechte erhöhen können.
- 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	0.986670000	Link
CVE-2023-42793	0.972640000	0.997920000	Link
CVE-2023-38035	0.970400000	0.996680000	Link
CVE-2023-35078	0.963850000	0.994100000	Link
CVE-2023-34362	0.921790000	0.986530000	Link
CVE-2023-33246	0.971460000	0.997250000	Link
CVE-2023-32315	0.954040000	0.991500000	Link
CVE-2023-30625	0.933370000	0.988040000	Link
CVE-2023-30013	0.936180000	0.988390000	Link
CVE-2023-28771	0.930510000	0.987660000	Link
CVE-2023-27524	0.912940000	0.985610000	Link
CVE-2023-27372	0.970490000	0.996730000	Link
CVE-2023-27350	0.971560000	0.997320000	Link
CVE-2023-26469	0.918080000	0.986110000	Link
CVE-2023-26360	0.913940000	0.985740000	Link
CVE-2023-25717	0.959190000	0.992750000	Link
CVE-2023-25194	0.910980000	0.985410000	Link
CVE-2023-2479	0.961630000	0.993340000	Link
CVE-2023-24489	0.969080000	0.996180000	Link
CVE-2023-22515	0.955290000	0.991830000	Link
CVE-2023-21839	0.960250000	0.993010000	Link
CVE-2023-21823	0.950040000	0.990630000	Link
CVE-2023-21554	0.961360000	0.993290000	Link
CVE-2023-20887	0.945440000	0.989940000	Link
CVE-2023-20198	0.955600000	0.991890000	Link
CVE-2023-0669	0.965820000	0.994810000	Link

BSI - Warn- und Informationsdienst (WID)

Thu, 02 Nov 2023

[NEU] [hoch] Cisco Adaptive Security Appliance & Firepower Threat Defense: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Cisco ASA (Adaptive Security Appliance) und Cisco Firepower ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 02 Nov 2023

[NEU] [hoch] Cisco Firepower Management Center: Mehrere Schwachstellen ermöglichen Cross-Site Scripting

Ein entfernter Angreifer kann mehrere Schwachstellen in Cisco Firepower Management Center ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- Link

—

Thu, 02 Nov 2023

[NEU] [hoch] Cisco Firepower Threat Defense Software und Management Center: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Cisco Firepower Threat Defense Software und Management Center ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Thu, 02 Nov 2023

[NEU] [hoch] Cisco Identity Services Engine (ISE): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Cisco Identity Services Engine (ISE) ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Thu, 02 Nov 2023

[NEU] [hoch] SolarWinds-Plattform: Schwachstelle ermöglicht die Ausführung von beliebigem Code mit Administratorrechten

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in SolarWinds Platform ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- Link

—

Thu, 02 Nov 2023

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

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

- Link

—

Thu, 02 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

—

Thu, 02 Nov 2023

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Thu, 02 Nov 2023

[UPDATE] [hoch] Red Hat Enterprise Linux (libvpx): Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Komponente libvpx ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- Link

—

Thu, 02 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

—

Thu, 02 Nov 2023

[UPDATE] [hoch] Xen: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Xen ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern.

- Link

—

Thu, 02 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

—

Thu, 02 Nov 2023

[UPDATE] [hoch] Mozilla Firefox 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 zu verursachen oder vertrauliche Informationen offenzulegen. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

- Link

—

Wed, 01 Nov 2023

[UPDATE] [hoch] libsndfile: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in libsndfile ausnutzen, um beliebigen Code auszuführen, einen 'Denial of Service'-Zustand herbeizuführen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Wed, 01 Nov 2023

[NEU] [hoch] SolarWinds Platform: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in SolarWinds Platform ausnutzen, um beliebigen Programmcode auszuführen und Sicherheitsmaßnahmen zu umgehen.

- Link

—

Wed, 01 Nov 2023

[NEU] [hoch] VMware Workspace One UEM: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Workspace One ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 01 Nov 2023

[NEU] [hoch] Nvidia Treiber: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Nvidia Treiber ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen, seine Privilegien zu erweitern und Daten zu manipulieren.

- Link

—

Wed, 01 Nov 2023

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, Informationen falsch darzustellen und Informationen offenzulegen.

- Link

—

Wed, 01 Nov 2023

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um einen Denial of Service Angriff durchzuführen und Informationen offenzulegen.

- Link

—

Wed, 01 Nov 2023

[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/2/2023	[F5 Networks BIG-IP : BIG-IP Engineering Hotfix authentication bypass vulnerability (K55655944)]	critical
11/2/2023	[F5 Networks BIG-IP : Rowhammer hardware vulnerability (K60570139)]	critical
11/2/2023	[F5 Networks BIG-IP : glibc vulnerability (K54823184)]	critical
11/2/2023	[F5 Networks BIG-IP : BIG-IP TMUI XSS vulnerability (K61643620)]	critical
11/2/2023	[Debian DLA-3644-1 : phppgadmin - LTS security update]	critical
11/2/2023	[Amazon Linux 2 : python (ALAS-2023-2330)]	critical
11/2/2023	[Amazon Linux 2 : zlib (ALAS-2023-2320)]	critical
11/2/2023	[F5 Networks BIG-IP : Multi-blade VIPRION Configuration utility session cookie vulnerability (K29141800)]	high
11/2/2023	[F5 Networks BIG-IP : SSL virtual server vulnerability (K45353544)]	high
11/2/2023	[F5 Networks BIG-IP : tcpdump vulnerability (K56551263)]	high
11/2/2023	[F5 Networks BIG-IP : TMM vulnerability (K70415522)]	high
11/2/2023	[F5 Networks BIG-IP : Expat XML parser vulnerability (K51011533)]	high
11/2/2023	[F5 Networks BIG-IP : IP Intelligence Feed List TMUI vulnerability (K68151373)]	high
11/2/2023	[F5 Networks BIG-IP : BIG-IP engineering hotfix TMM vulnerability (K53590702)]	high
11/2/2023	[F5 Networks BIG-IP : BIG-IP DNS vulnerability (K43850230)]	high
11/2/2023	[F5 Networks BIG-IP : BIG-IP network failover vulnerability (K67472032)]	high
11/2/2023	[F5 Networks BIG-IP : iRules RESOLVER::summarize memory leak vulnerability (K65397301)]	high
11/2/2023	[F5 Networks BIG-IP : Linux kernel vulnerability (K40540405)]	high
11/2/2023	[F5 Networks BIG-IP : iControl SOAP vulnerability (K53854428)]	high
11/2/2023	[F5 Networks BIG-IP : NTP vulnerability (K44305703)]	high
11/2/2023	[F5 Networks BIG-IP : BIG-IP DNS vulnerability (K45407662)]	high
11/2/2023	[F5 Networks BIG-IP : glibc vulnerability (K49921213)]	high
11/2/2023	[F5 Networks BIG-IP : LibTIFF vulnerability (K70117303)]	high
11/2/2023	[F5 Networks BIG-IP : libarchive vulnerability (K50543013)]	high
11/2/2023	[RHEL 9 : c-ares (RHSA-2023:6291)]	high
11/2/2023	[Amazon Linux 2 : kernel (ALAS-2023-2328)]	high
11/2/2023	[Amazon Linux 2 : vim (ALAS-2023-2319)]	high
11/2/2023	[Amazon Linux 2 : httpd (ALAS-2023-2322)]	high
11/2/2023	[Amazon Linux 2 : cri-tools (ALAS-2023-2324)]	high
11/2/2023	[Amazon Linux 2 : open-vm-tools (ALAS-2023-2329)]	high
11/2/2023	[Amazon Linux 2 : nmap (ALAS-2023-2333)]	high
11/2/2023	[Amazon Linux 2 : cni-plugins (ALAS-2023-2325)]	high
11/2/2023	[Amazon Linux 2 : xerces-c (ALAS-2023-2327)]	high
11/2/2023	[Amazon Linux 2 : libguestfs-winsupport (ALAS-2023-2332)]	high
11/2/2023	[Amazon Linux 2 : golist (ALAS-2023-2326)]	high
11/2/2023	[Amazon Linux 2 : opensc (ALAS-2023-2323)]	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

“Thu, 02 Nov 2023

ZDI-23-1581: (0Day) Microsoft Exchange CreateAttachmentFromUri Server-Side Request Forgery Information Disclosure Vulnerability

- Link

—

” “Thu, 02 Nov 2023

ZDI-23-1580: (0Day) Microsoft Exchange DownloadDataFromOfficeMarketPlace Server-Side Request Forgery Information Disclosure Vulnerability

- Link

—

” “Thu, 02 Nov 2023

ZDI-23-1579: (0Day) Microsoft Exchange DownloadDataFromUri Server-Side Request Forgery Information Disclosure Vulnerability

- Link

—

” “Thu, 02 Nov 2023

ZDI-23-1578: (0Day) Microsoft Exchange ChainedSerializationBinder Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—
”

Die Hacks der Woche

mit Martin Haunschmid

Ist jetzt der nächste Passwortmanager dran? 1Password-HACK

Zum Youtube Video

Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2023-11-01	Mr. Cooper Group	[USA]	Link

Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.