



Ausgabe: 20231012

# 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

### *Patchday F5: Sicherheitslücken in BIG-IP ermöglichen Angreifern Codeausführung*

F5 hat mehrere Sicherheitsmeldungen zu Lecks in BIG-IP-Appliances und -Software veröffentlicht. Aktualisierungen stehen bereit.

- [Link](#)

---

### *Sicherheitsupdates Fortinet: Angreifer können Passwörter im Klartext einsehen*

Fortinet hat wichtige Sicherheitspatches für FortiOS und FortiProxy veröffentlicht.

- [Link](#)

---

### *Rapid Reset: Angreifer nutzen Lücke im HTTP/2-Protokoll seit August 2023 aus*

Eine DDoS-Sicherheitslücke mit Rekordvolumen im HTTP/2-Protokoll gefährdet unzählige Server. Erste Sicherheitspatches sind verfügbar.

- [Link](#)

---

### *Citrix dichtet kritisches Leck in Netscaler ab*

In Netscaler ADC und Gateway klaffen Sicherheitslücken, ebenso im Hypervisor von Citrix. Aktualisierte Software-Pakete schließen sie.

- [Link](#)

---

### *Patchday Adobe: Schadcode-Attacken auf Magento-Shops und Photoshop möglich*

Die Entwickler von Adobe haben in Bridge, Commerce, Magento Open Source und Photoshop mehrere Sicherheitslücken geschlossen.

- [Link](#)

---

### *Webbrowser: Google-Chrome-Update schließt kritische Sicherheitslücke*

Google hat das wöchentliche Chrome-Update herausgegeben. Es schließt 20 Sicherheitslücken, von denen mindestens eine als kritisch gilt.

- [Link](#)

---

### *Patchday Microsoft: Attacken auf Skype for Business und WordPad*

Microsoft hat wichtige Sicherheitsupdates für etwa Azure, Office und Windows veröffentlicht.

- [Link](#)

---

### *libcve-Lücke reißt Sicherheitsleck in Gnome*

Eine Schwachstelle in einer unscheinbaren Bibliothek führt zu einer veritablen Sicherheitslücke in Gnome. Updates stehen bereit.

- [Link](#)

---

### *Sicherheitsupdates: Schadcode- und Root-Lücken bedrohen IBM-Software*

IBM hat unter anderem im Datenbankmanagementsystem Db2 schwerwiegende Schwachstellen geschlossen.

- [Link](#)

---

### *Backup: Acronis schließt Sicherheitslücken im Agent für Linux, Mac und Windows*

Acronis hat eine Aktualisierung des Agent für Linux, Mac und Windows veröffentlicht. Sie dichtet unter anderem ein Leck mit hohem Risiko ab.

- [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-2023-42793	0.972090000	0.997570000	<a href="#">Link</a>
CVE-2023-38035	0.970820000	0.996860000	<a href="#">Link</a>
CVE-2023-35078	0.959430000	0.992650000	<a href="#">Link</a>
CVE-2023-34362	0.921790000	0.986240000	<a href="#">Link</a>
CVE-2023-33246	0.971460000	0.997200000	<a href="#">Link</a>
CVE-2023-32315	0.960720000	0.992990000	<a href="#">Link</a>
CVE-2023-30625	0.932650000	0.987720000	<a href="#">Link</a>
CVE-2023-30013	0.936180000	0.988180000	<a href="#">Link</a>
CVE-2023-28771	0.926550000	0.986850000	<a href="#">Link</a>
CVE-2023-27524	0.932860000	0.987780000	<a href="#">Link</a>
CVE-2023-27372	0.971800000	0.997420000	<a href="#">Link</a>
CVE-2023-27350	0.971270000	0.997100000	<a href="#">Link</a>
CVE-2023-26469	0.918080000	0.985830000	<a href="#">Link</a>
CVE-2023-26360	0.919780000	0.986030000	<a href="#">Link</a>
CVE-2023-25717	0.961530000	0.993170000	<a href="#">Link</a>
CVE-2023-25194	0.924830000	0.986610000	<a href="#">Link</a>
CVE-2023-2479	0.964610000	0.994190000	<a href="#">Link</a>
CVE-2023-24489	0.967770000	0.995500000	<a href="#">Link</a>
CVE-2023-22515	0.935270000	0.988080000	<a href="#">Link</a>
CVE-2023-21839	0.951010000	0.990690000	<a href="#">Link</a>
CVE-2023-21823	0.929300000	0.987250000	<a href="#">Link</a>
CVE-2023-21554	0.961360000	0.993140000	<a href="#">Link</a>
CVE-2023-20887	0.932820000	0.987770000	<a href="#">Link</a>
CVE-2023-0669	0.968230000	0.995640000	<a href="#">Link</a>

---

## BSI - Warn- und Informationsdienst (WID)

Wed, 11 Oct 2023

**[UPDATE] [hoch] cURL: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um Sicherheitsvorkehrungen zu umgehen und einen Denial of Service Zustand herzustellen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Fortinet FortiManager und Fortinet FortiAnalyzer: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Fortinet FortiManager und Fortinet FortiAnalyzer ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder Dateien zu manipulieren.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Red Hat Enterprise Linux (python-reportlab): Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente "python-reportlab" ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Wed, 11 Oct 2023

**[UPDATE] [hoch] F5 BIG-IP: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in F5 BIG-IP ausnutzen, um beliebigen Code auszuführen, seine Privilegien zu erhöhen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [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, 11 Oct 2023

**[NEU] [kritisch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen und Privilegien zu erweitern.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Eclipse Jetty: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Eclipse Jetty ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Fortinet FortiOS: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Fortinet FortiOS ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

---

Wed, 11 Oct 2023

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

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

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in IBM QRadar

SIEM ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

---

Wed, 11 Oct 2023

**[UPDATE] [UNGEPATCHT] [hoch] D-LINK DIR-X3260 Router: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im D-LINK Router ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Adobe Magento: Mehrere Schwachstellen**

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Adobe Magento ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [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, 11 Oct 2023

**[NEU] [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](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Fortinet FortiMail: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Fortinet FortiMail ausnutzen, um Sicherheitsvorkehrungen zu umgehen und Daten zu manipulieren.

- [Link](#)

---

Wed, 11 Oct 2023

**[UPDATE] [hoch] GNOME: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Azure, Microsoft Azure DevOps Server und Microsoft Azure RTOS ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code zur Ausführung zu bringen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Microsoft Exchange Server: Schwachstelle ermöglicht Codeausführung**

Ein Angreifer kann eine Schwachstelle in Microsoft Exchange Server ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Wed, 11 Oct 2023

**[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Office ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- [Link](#)

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/11/2023	[Dell EMC iDRAC9 4.40.00.00 < 4.40.10.00 (DSA-2021-082)]	critical
10/11/2023	[Juniper Junos OS Multiple Vulnerabilities (JSA73176)]	critical
10/11/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:4033-1)]	high
10/11/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:4035-1)]	high
10/11/2023	[SUSE SLES15 / openSUSE 15 Security Update : common (SUSE-SU-2023:4022-1)]	high
10/11/2023	[SUSE SLES15 / openSUSE 15 Security Update : common (SUSE-SU-2023:4042-1)]	high
10/11/2023	[SUSE SLED12 / SLES12 Security Update : kernel (SUSE-SU-2023:4031-1)]	high
10/11/2023	[SUSE SLES15 Security Update : kernel (SUSE-SU-2023:4030-1)]	high
10/11/2023	[SUSE SLES15 / openSUSE 15 Security Update : php-composer2 (SUSE-SU-2023:4041-1)]	high
10/11/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:4032-1)]	high
10/11/2023	[SUSE SLES15 Security Update : common (SUSE-SU-2023:4021-1)]	high
10/11/2023	[Oracle Linux 7 : kernel (ELSA-2023-5622)]	high
10/11/2023	[Oracle Linux 9 : libvpx (ELSA-2023-5539)]	high
10/11/2023	[FreeBSD : curl – SOCKS5 heap buffer overflow (d6c19e8c-6806-11ee-9464-b42e991fc52e)]	high
10/11/2023	[Adobe Photoshop 23.x < 24.7.1 / 24.x < 24.7.1 Vulnerability (APSB23-51)]	high
10/11/2023	[Adobe Photoshop 23.x < 24.7.1 / 24.x < 24.7.1 Vulnerability (macOS APSB23-51)]	high
10/11/2023	[Security Update for .NET Core SDK (October 2023)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73163)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73141)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73158)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73156)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73172)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73165)]	high
10/11/2023	[Juniper Junos OS Vulnerability (JSA73155)]	high

# Aktiv ausgenutzte Sicherheitslücken

## Exploits

“Wed, 11 Oct 2023

### ***Smart School 6.4.1 SQL Injection***

Smart School version 6.4.1 suffers from multiple remote SQL injection vulnerabilities.

- [Link](#)

---

” “Wed, 11 Oct 2023

### ***Gaatitrack 1.0-2023 SQL Injection***

Gaatitrack version 1.0-2023 suffers from a remote SQL injection vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***Cacti 1.2.24 Command Injection***

Cacti version 1.2.24 authenticated command injection exploit that uses SNMP options.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***BoidCMS 2.0.0 Shell Upload***

BoidCMS versions 2.0.0 and below suffer from a remote shell upload vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***Webedition CMS 2.9.8.8 Server-Side Request Forgery***

Webedition CMS version 2.9.8.8 suffers from a blind server-side request forgery vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***OpenPLC WebServer 3 Denial Of Service***

OpenPLC WebServer version 3 suffers from a denial of service vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***Atcom 2.7.x.x Command Injection***

Atcom version 2.7.x.x suffers from an authenticated remote code injection vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***WordPress Sonaar Music 4.7 Cross Site Scripting***

WordPress Sonaar Music plugin version 4.7 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***Coppermine Gallery 1.6.25 Remote Code Execution***

Coppermine Gallery version 1.6.25 remote code execution exploit.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***Minio 2022-07-29T19-40-48Z Path Traversal***

Minio version 2022-07-29T19-40-48Z suffers from a path traversal vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023

### ***WordPress Masterstudy LMS 3.0.17 Account Creation***

WordPress Masterstudy LMS plugin version 3.0.17 suffers from an unauthenticated instructor account creation vulnerability.

- [Link](#)

---

” “Tue, 10 Oct 2023



***Microsoft Windows 11 apds.dll DLL Hijacking***

Microsoft Windows 11 apds.dll DLL hijacking exploit.

- [Link](#)

---

” “Tue, 10 Oct 2023

***GLPI GZIP(Py3) 9.4.5 Remote Code Execution***

GLPI GZIP(Py3) version 9.4.5 suffers from a remote code execution vulnerability.

- [Link](#)

---

” “Mon, 09 Oct 2023

***Kibana Prototype Pollution / Remote Code Execution***

Kibana versions prior to 7.6.3 suffer from a prototype pollution bug within the Upgrade Assistant. By setting a new constructor.prototype.sourceURL value you can execute arbitrary code. Code execution is possible through two different ways. Either by sending data directly to Elastic, or using Kibana to submit the same queries. Either method enters the polluted prototype for Kibana to read. Kibana will either need to be restarted, or collection happens (unknown time) for the payload to execute. Once it does, cleanup must delete the .kibana\_1 index for Kibana to restart successfully. Once a callback does occur, cleanup will happen allowing Kibana to be successfully restarted on next attempt.

- [Link](#)

---

” “Mon, 09 Oct 2023

***eClass Junior 4.0 SQL Injection***

eClass Junior version 4.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

---

” “Mon, 09 Oct 2023

***eClass IP 2.5 SQL Injection***

eClass IP version 2.5 suffers from a remote SQL injection vulnerability.

- [Link](#)

---

” “Mon, 09 Oct 2023

***Chicv Management System Login 4.5.6 Insecure Direct Object Reference***

Chicv Management System Login version 4.5.6 suffers from an insecure direct object reference vulnerability.

- [Link](#)

---

” “Mon, 09 Oct 2023

***Aicte India LMS 3.0 Cross Site Scripting***

Aicte India LMS version 3.0 suffers from a cross site scripting vulnerability.

- [Link](#)

---

” “Fri, 06 Oct 2023

***glibc ld.so Local Privilege Escalation***

Dubbed Looney Tunables, Qualys discovered a buffer overflow vulnerability in the glibc dynamic loader’s processing of the GLIBC\_TUNABLES environment variable. This vulnerability was introduced in April 2021 (glibc 2.34) by commit 2ed18c.

- [Link](#)

---

” “Fri, 06 Oct 2023

***SAP Application Server ABAP Open Redirection***

SAP Application Server ABAP and ABAP Platform suffer from an open redirection vulnerability.

- [Link](#)

---

” “Thu, 05 Oct 2023

***Chrome ReduceJSLoadPropertyWithEnumeratedKey Out-Of-Bounds Access***

Chrome checks in ReduceJSLoadPropertyWithEnumeratedKey are not sufficient to prevent the engine from reading an out-of-bounds index from an enum cache.

- [Link](#)

---

” “Thu, 05 Oct 2023

***Chrome Dangling FixedArray Pointers / Memory Corruption***

Chrome suffers from an issue with dangling FixedArray pointers in Torque that can lead to memory corruption.

- [Link](#)

---

” “Thu, 05 Oct 2023

***Chrome SKIA Integer Overflow***

When deserializing an SkPath, there is some basic validation performed to ensure that the contents are consistent. This validation does not use safe integer types, or perform additional validation, so it’s possible for a large path to overflow the point count, resulting in an unsafe SkPath object.

- [Link](#)

---

” “Thu, 05 Oct 2023

***edgetpu\_pin\_user\_pages Race Condition***

There is a race condition in edgetpu\_pin\_user\_pages which is reachable from some unprivileged contexts, including the Camera app, or the Google Meet app.

- [Link](#)

---

” “Wed, 04 Oct 2023

***Progress Software WS\_FTP Unauthenticated Remote Code Execution***

This Metasploit module exploits an unsafe .NET deserialization vulnerability to achieve unauthenticated remote code execution against a vulnerable WS\_FTP server running the Ad Hoc Transfer module. All versions of WS\_FTP Server prior to 2020.0.4 (version 8.7.4) and 2022.0.2 (version 8.8.2) are vulnerable to this issue. The vulnerability was originally discovered by AssetNote.

- [Link](#)

---

”

## 0-Day

“Wed, 11 Oct 2023

***ZDI-23-1558: Siemens Tecnomatix Plant Simulation PAR File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

***ZDI-23-1557: Siemens Tecnomatix Plant Simulation PRT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

***ZDI-23-1556: Siemens Tecnomatix Plant Simulation PAR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

***ZDI-23-1555: Microsoft Windows DirectX GpuMmu Race Condition Local Privilege Escalation Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

***ZDI-23-1554: Microsoft Windows bStretch Improper Input Validation Local Privilege Escalation Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

***ZDI-23-1553: Microsoft Windows DEVLOCKBLTOBJ Race Condition Local Privilege Escalation Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

***ZDI-23-1552: Microsoft Windows UMPDDrvPlgBlT Type Confusion Local Privilege Escalation Vulnerability***

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1551: Microsoft Windows UMPDDrvStretchBlt Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1550: Microsoft Windows UMPDDrvBitBlt Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1549: Microsoft Windows UMPDDrvStretchBltROP Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1548: Microsoft Windows UMPDDrvCopyBits Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1547: Microsoft Windows UMPDDrvStretchBlt Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1546: Microsoft Windows UMPDDrvStretchBltROP Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1545: Microsoft Windows IsSurfaceLockable Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1544: Microsoft Windows UMPDDrvPlgBlt Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1543: Microsoft Windows UMPDDrvBitBlt Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1542: Microsoft Windows UMPDDrvCopyBits Type Confusion Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1541: (Pwn2Own) Microsoft Teams Incorrect Privilege Assignment Local Privilege Escalation Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1540: (Pwn2Own) Microsoft Teams Cross-Site Scripting Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1539: Adobe Photoshop PSD File Parsing Uninitialized Variable Remote Code Execution Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1538: Adobe Bridge Font Parsing Out-Of-Bounds Read Information Disclosure Vulnerability*

- [Link](#)

---

” “Wed, 11 Oct 2023

*ZDI-23-1537: Adobe Bridge Font Parsing Use-After-Free Information Disclosure Vulnerability*

- [Link](#)

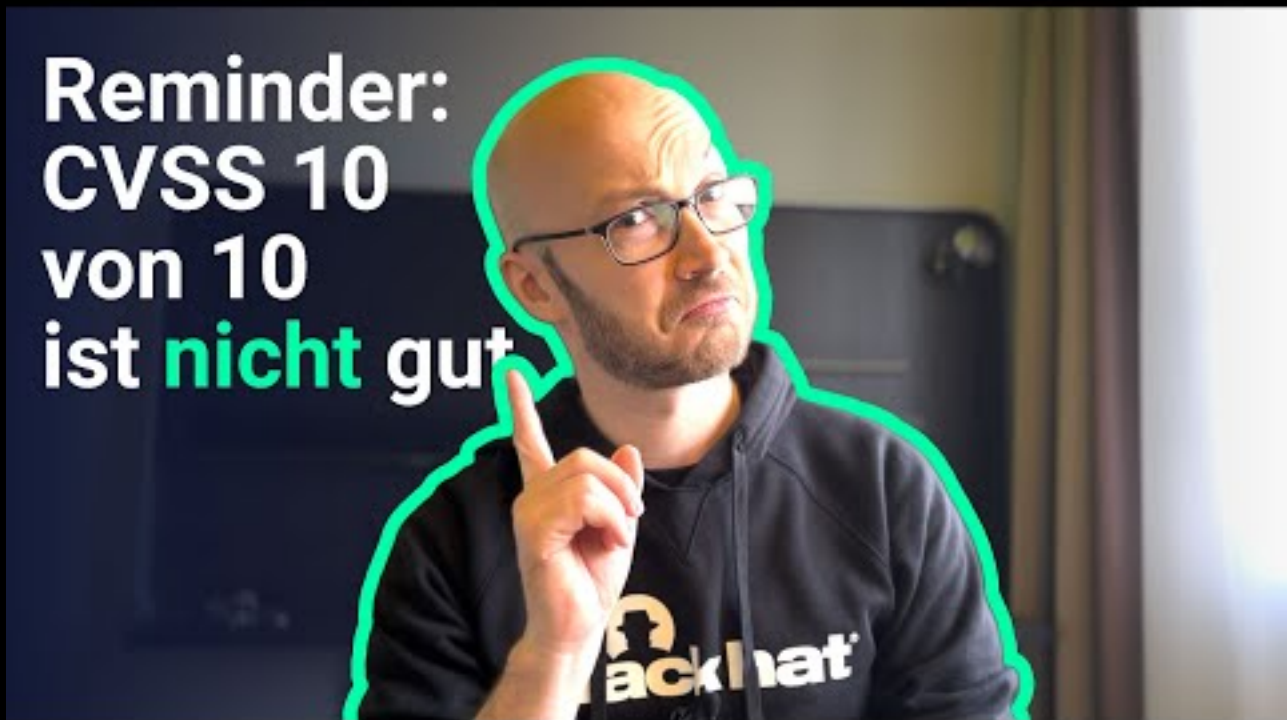
---

”

## Die Hacks der Woche

mit Martin Haunschmid

In der IT-Security ist 10 von 10 NICHT IMMER etwas Gutes



[Zum Youtube Video](#)

## Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2023-10-10	Simpson Manufacturing Co.	[USA]	<a href="#">Link</a>
2023-10-09	De La Salle University (DLSU)	[PHL]	<a href="#">Link</a>
2023-10-08	Volex PLC	[GBR]	<a href="#">Link</a>
2023-10-07	Centre hospitalier de l'Ouest Vosgien	[FRA]	<a href="#">Link</a>
2023-10-06	Clinique universitaire de Francfort	[DEU]	<a href="#">Link</a>
2023-10-05	Dansk Scanning	[DNK]	<a href="#">Link</a>
2023-10-03	Metro Transit	[USA]	<a href="#">Link</a>
2023-10-02	Estes Express Lines	[USA]	<a href="#">Link</a>
2023-10-02	Hochschule de Karlsruhe	[DEU]	<a href="#">Link</a>
2023-10-02	Provincia di Cosenza	[ITA]	<a href="#">Link</a>
2023-10-02	Degenia	[DEU]	<a href="#">Link</a>
2023-10-02	Le Premier Circuit Judiciaire de Floride	[USA]	<a href="#">Link</a>
2023-10-01	Lyca Mobile UK	[GBR]	<a href="#">Link</a>

## Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-11	[Scotbeef Ltd. - Leaks]	ragnarlocker	<a href="#">Link</a>
2023-10-09	[LDLC ASVEL]	noescape	<a href="#">Link</a>
2023-10-11	[Institut Technologique FCBA]	alphv	<a href="#">Link</a>
2023-10-09	[Instant Access Co]	noescape	<a href="#">Link</a>
2023-10-11	[Eicon Controle Inteligentes]	ragnarlocker	<a href="#">Link</a>
2023-10-11	[Air Canada]	bianlian	<a href="#">Link</a>
2023-10-11	[Pelindo]	bianlian	<a href="#">Link</a>
2023-10-11	[Instron & ITW Inc]	bianlian	<a href="#">Link</a>
2023-10-11	[Mid-America Real Estate Group]	alphv	<a href="#">Link</a>
2023-10-11	[Village Building Co.]	incransom	<a href="#">Link</a>
2023-10-11	[STANTONWILLIAMS]	blackbasta	<a href="#">Link</a>
2023-10-11	[REH]	blackbasta	<a href="#">Link</a>
2023-10-11	[HAEFFNER-ASP]	blackbasta	<a href="#">Link</a>
2023-10-11	[GREGAGG]	blackbasta	<a href="#">Link</a>
2023-10-11	[Catarineau & Givens P.A]	alphv	<a href="#">Link</a>
2023-10-11	[Sobieski]	incransom	<a href="#">Link</a>
2023-10-11	[We monetize your corporate access]	everest	<a href="#">Link</a>
2023-10-09	[Metro Transit]	play	<a href="#">Link</a>
2023-10-01	[Effigest Capital Services]	noescape	<a href="#">Link</a>
2023-10-10	[Alliance Virgil Roberts Leadership Academy]	snatch	<a href="#">Link</a>
2023-10-10	[foremostgroups.com]	lockbit3	<a href="#">Link</a>
2023-10-10	[National Health Mission. Department of Health & Family Welfare, Govt. of U.P]	knight	<a href="#">Link</a>
2023-10-10	[mountstmarys]	cuba	<a href="#">Link</a>
2023-10-10	[ExdionInsurance]	8base	<a href="#">Link</a>
2023-10-10	[National Health Mission. Department of Heath & Family Welfare, Govt. of U.P]	knight	<a href="#">Link</a>
2023-10-01	[Elbe-Obst Fruchtverarbeitung GmbH]	noescape	<a href="#">Link</a>
2023-10-03	[Ordine Degli Psicologi Della Lombardia]	noescape	<a href="#">Link</a>
2023-10-09	[Saltire Energy]	play	<a href="#">Link</a>
2023-10-09	[Starr Finley]	play	<a href="#">Link</a>
2023-10-09	[WCM Europe]	play	<a href="#">Link</a>
2023-10-09	[NachtExpress Austria GmbH]	play	<a href="#">Link</a>
2023-10-09	[Centek industries]	play	<a href="#">Link</a>
2023-10-09	[M??? T??????]	play	<a href="#">Link</a>
2023-10-10	[Hughes Gill Cochrane Tinetti]	play	<a href="#">Link</a>
2023-10-01	[Penfield Fire Co]	noescape	<a href="#">Link</a>
2023-10-01	[Centre Du Sablon]	noescape	<a href="#">Link</a>
2023-10-06	[GEACAM]	noescape	<a href="#">Link</a>
2023-10-09	[Guhring was hacked. Thousands of confidential files stolen.]	knight	<a href="#">Link</a>
2023-10-09	[Wyndemere Senior Care, LLC]	alphv	<a href="#">Link</a>
2023-10-09	[First Judicial Circuit - Florida Court]	alphv	<a href="#">Link</a>
2023-10-09	[atlantatech.edu]	lockbit3	<a href="#">Link</a>
2023-10-09	[starplast.ft]	lockbit3	<a href="#">Link</a>
2023-10-09	[WT PARTNERSHIP]	qilin	<a href="#">Link</a>
2023-10-09	[Superline - Press Release]	monti	<a href="#">Link</a>
2023-10-09	[dothanhauto.com]	lockbit3	<a href="#">Link</a>
2023-10-09	[vsmpto-tirus.com]	lockbit3	<a href="#">Link</a>
2023-10-09	[Law Society of South Africa]	alphv	<a href="#">Link</a>
2023-10-09	[enerjet.com.pe]	lockbit3	<a href="#">Link</a>
2023-10-09	[i-Can Advisory Group inc]	alphv	<a href="#">Link</a>
2023-10-09	[BrData Tecnologia]	alphv	<a href="#">Link</a>
2023-10-09	[Southern Arkansas University]	rhysida	<a href="#">Link</a>
2023-10-08	[securicon.co.za]	lockbit3	<a href="#">Link</a>
2023-10-08	[Islamic Azad University of Shiraz]	arvinclub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-08	[urc-automation.com]	lockbit3	Link
2023-10-08	[IKM]	alphv	<a href="#">Link</a>
2023-10-08	[Petersen Johnson]	8base	Link
2023-10-07	[University Obrany - Part 2 (Tiny Leak)]	monti	Link
2023-10-07	[DallBogg Breach]	ransomed	Link
2023-10-07	[Partnership With Breachforums]	ransomed	Link
2023-10-07	[The Hurley Group]	cactus	Link
2023-10-07	[Healix]	akira	Link
2023-10-06	[International Presence Ltd - Leaked]	ragnarlocker	Link
2023-10-06	[For UNOB]	monti	Link
2023-10-04	[NTT Docomo]	ransomed	Link
2023-10-05	[(SALE) District Of Columbia Elections 600k lines VOTERS DATA]	ransomed	Link
2023-10-06	[Agència Catalana de Notícies (ACN)]	medusa	Link
2023-10-06	[cote-expert-equipements.com]	lockbit3	Link
2023-10-06	[sinediadvisor.com]	lockbit3	Link
2023-10-06	[tatatelebusiness.com]	lockbit3	Link
2023-10-06	[eemotors.com]	lockbit3	Link
2023-10-06	[bm.co.th]	lockbit3	Link
2023-10-06	[picosoft.biz]	lockbit3	Link
2023-10-06	[litung.com.tw]	lockbit3	Link
2023-10-05	[Granger Medical Clinic]	noescape	<a href="#">Link</a>
2023-10-06	[Camara Municipal de Gondomar]	rhysida	Link
2023-10-05	[sirva.com]	lockbit3	Link
2023-10-05	[Low Keng Huat (Singapore) Limited]	bianlian	Link
2023-10-05	[Cornerstone Projects Group]	cactus	Link
2023-10-05	[RICOR Global Limited]	cactus	Link
2023-10-05	[Learning Partnership West - Leaked]	ragnarlocker	Link
2023-10-05	[Terwilliger Land Survey Engineers]	akira	Link
2023-10-04	[DiTRONICS Financial Services]	qilin	<a href="#">Link</a>
2023-10-04	[suncoast-chc.org]	lockbit3	Link
2023-10-04	[Meridian Cooperative]	blackbyte	<a href="#">Link</a>
2023-10-04	[Roof Management]	play	<a href="#">Link</a>
2023-10-04	[Security Instrument]	play	<a href="#">Link</a>
2023-10-04	[Filtration Control]	play	<a href="#">Link</a>
2023-10-04	[Cinepolis USA]	play	<a href="#">Link</a>
2023-10-04	[CHARMANT Group]	play	<a href="#">Link</a>
2023-10-04	[Stavanger Municipality]	play	<a href="#">Link</a>
2023-10-04	[Gruskin Group]	akira	Link
2023-10-04	[McLaren Health Care Corporation]	alphv	<a href="#">Link</a>
2023-10-04	[US Liner Company & American Made LLC]	0mega	Link
2023-10-04	[General Directorate of Migration of the Dominican Republic]	rhysida	Link
2023-10-03	[University of Defence - Part 1]	monti	Link
2023-10-03	[Toscana Promozione]	moneymessage	Link
2023-10-03	[MD LOGISTICS]	moneymessage	Link
2023-10-03	[Maxco Supply]	moneymessage	Link
2023-10-03	[Groupe Fructa Partner - Leaked]	ragnarlocker	Link
2023-10-03	[Somagic]	medusa	Link
2023-10-03	[The One Group]	alphv	<a href="#">Link</a>
2023-10-03	[aicsacorp.com]	lockbit3	Link
2023-10-03	[co.rock.wi.us]	cuba	Link
2023-10-03	[Sabian Inc]	8base	Link
2023-10-03	[Ted Pella Inc.]	8base	Link
2023-10-03	[GDL Logística Integrada S.A]	knight	Link
2023-10-03	[Measuresoft]	mallox	Link
2023-10-02	[RAT.]	donutleaks	Link
2023-10-02	[AllCare Pharmacy]	lorenz	<a href="#">Link</a>
2023-10-02	[Confidential files]	medusalocker	Link



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-02	[Pain Care]	alphv	<a href="#">Link</a>
2023-10-02	[Windak]	medusa	<a href="#">Link</a>
2023-10-02	[Pasouk biological company]	arvinclub	<a href="#">Link</a>
2023-10-02	[Karam Chand Thapar & Bros Coal Sales]	medusa	<a href="#">Link</a>
2023-10-02	[Kirkholm Maskiningeniører]	mallox	<a href="#">Link</a>
2023-10-02	[Federal University of Mato Grosso do Sul]	rhysida	<a href="#">Link</a>
2023-10-01	[erga.com]	lockbit3	<a href="#">Link</a>
2023-10-01	[thermae.nl]	lockbit3	<a href="#">Link</a>
2023-10-01	[ckgroup.com.tw]	lockbit3	<a href="#">Link</a>
2023-10-01	[raeburns.co.uk]	lockbit3	<a href="#">Link</a>
2023-10-01	[tayloredservices.com]	lockbit3	<a href="#">Link</a>
2023-10-01	[fcps1.org]	lockbit3	<a href="#">Link</a>
2023-10-01	[laspesainfamiglia.coop]	lockbit3	<a href="#">Link</a>
2023-10-01	[Cascade Family Dental - Press Release]	monti	<a href="#">Link</a>
2023-10-01	[Rainbow Travel Service - Press Release]	monti	<a href="#">Link</a>
2023-10-01	[Shirin Travel Agency]	arvinclub	<a href="#">Link</a>
2023-10-01	[Flamingo Holland]	trigona	<a href="#">Link</a>
2023-10-01	[Aria Care Partners]	trigona	<a href="#">Link</a>
2023-10-01	[Portesa]	trigona	<a href="#">Link</a>
2023-10-01	[Grupo Boreal]	trigona	<a href="#">Link</a>
2023-10-01	[Quest International]	trigona	<a href="#">Link</a>
2023-10-01	[Arga Medicali]	alphv	<a href="#">Link</a>

# 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](https://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](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.