



Ausgabe: 20231031

# 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

### *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](#)

---

### *Rechteauserweiterung durch Lücke in HP Print and Scan Doctor*

Aktualisierte Software korrigiert einen Fehler im Support-Tool HP Print and Scan Doctor, der die Ausweitung der Rechte im System ermöglicht.

- [Link](#)

---

### *Sicherheitslücken im X.Org X-Server und Xwayland erlauben Rechteauserweiterung*

Aktualisierte Fassung des X.Org X-Servers und von Xwayland schließen Sicherheitslücken. Die erlauben die Rechteauserweiterung oder einen Denial-of-Service.

- [Link](#)

---

### *Sicherheitsupdates: Jenkins-Plug-ins als Einfallstor für Angreifer*

Jenkins kann bei der Softwareentwicklung helfen. Einige Plug-ins weisen Sicherheitslücken auf. Ein paar Updates stehen noch aus.

- [Link](#)

---

### *Teils kritische Lücken in VMware vCenter Server und Cloud Foundation geschlossen*

VMware hat aktualisierte Softwarepakete veröffentlicht, die mehrere Lücken in vCenter Server und Cloud Foundation abdichten. Eine gilt als kritisch.

- [Link](#)

---

### *Webmailer Roundcube: Attacken auf Zero-Day-Lücke*

Im Webmailer Roundcube missbrauchen Cyberkriminelle eine Sicherheitslücke, um verwundbare Einrichtungen anzugreifen. Ein Update schließt das Leck.

- [Link](#)

---

### *Exploitcode für Root-Lücke in VMware Aria Operations for Logs in Umlauf*

In Umlauf befindlicher Exploitcode gefährdet VMwares Management-Plattform für Cloudumgebungen. Admins sollten jetzt Sicherheitsupdates installieren.

- [Link](#)

---

### *Webbrowser: Google-Chrome-Update schließt zwei Sicherheitslücken*

Mit dem jetzt erschienenen Update bessern die Entwickler von Google Chrome zwei Schwachstellen aus. Webseiten können vermutlich Schadcode einschleusen.

- [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	0.972640000	0.997920000	<a href="#">Link</a>
CVE-2023-38035	0.970400000	0.996680000	<a href="#">Link</a>
CVE-2023-35078	0.961280000	0.993250000	<a href="#">Link</a>
CVE-2023-34362	0.921790000	0.986480000	<a href="#">Link</a>
CVE-2023-33246	0.971460000	0.997240000	<a href="#">Link</a>
CVE-2023-32315	0.954040000	0.991480000	<a href="#">Link</a>
CVE-2023-30625	0.933370000	0.988000000	<a href="#">Link</a>
CVE-2023-30013	0.936180000	0.988360000	<a href="#">Link</a>
CVE-2023-28771	0.930510000	0.987620000	<a href="#">Link</a>
CVE-2023-27524	0.912940000	0.985570000	<a href="#">Link</a>
CVE-2023-27372	0.970490000	0.996720000	<a href="#">Link</a>
CVE-2023-27350	0.971560000	0.997320000	<a href="#">Link</a>
CVE-2023-26469	0.918080000	0.986050000	<a href="#">Link</a>
CVE-2023-26360	0.913940000	0.985700000	<a href="#">Link</a>
CVE-2023-25717	0.959190000	0.992720000	<a href="#">Link</a>
CVE-2023-25194	0.910980000	0.985380000	<a href="#">Link</a>
CVE-2023-2479	0.961630000	0.993330000	<a href="#">Link</a>
CVE-2023-24489	0.969080000	0.996150000	<a href="#">Link</a>
CVE-2023-22515	0.955290000	0.991810000	<a href="#">Link</a>
CVE-2023-21839	0.952950000	0.991210000	<a href="#">Link</a>
CVE-2023-21823	0.950040000	0.990600000	<a href="#">Link</a>
CVE-2023-21554	0.961360000	0.993280000	<a href="#">Link</a>
CVE-2023-20887	0.945440000	0.989910000	<a href="#">Link</a>
CVE-2023-0669	0.965820000	0.994800000	<a href="#">Link</a>

---

## BSI - Warn- und Informationsdienst (WID)

Mon, 30 Oct 2023

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um einen Denial of Service Angriff durchzuführen, einen Cross-Site-Scripting-Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

---

Mon, 30 Oct 2023

**[UPDATE] [hoch] UnZip: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in UnZip ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Mon, 30 Oct 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](#)

---

Mon, 30 Oct 2023

**[UPDATE] [hoch] SugarCRM Sugar Enterprise: Mehrere Schwachstellen**

Ein entfernter authentisierter Angreifer kann mehrere Schwachstellen in SugarCRM Sugar Enterprise ausnutzen, um beliebigen Code auszuführen.

- [Link](#)

---

Mon, 30 Oct 2023

**[NEU] [hoch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

---

Mon, 30 Oct 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](#)

---

Mon, 30 Oct 2023

**[UPDATE] [hoch] Apache log4j: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache log4j ausnutzen, um beliebigen Programmcode auszuführen oder einen SQL-Injection durchzuführen.

- [Link](#)

---

Mon, 30 Oct 2023

**[UPDATE] [hoch] Grub2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff**

Ein Angreifer kann mehrere Schwachstellen in Oracle Linux ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

---

Mon, 30 Oct 2023

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand zu verursachen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen verursachen.

- [Link](#)

---

Mon, 30 Oct 2023

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Mon, 30 Oct 2023

**[UPDATE] [kritisch] Exim: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Exim ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

---

Mon, 30 Oct 2023

**[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen**

Ein entfernter, anonymen 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](#)

---

Mon, 30 Oct 2023

**[NEU] [hoch] Microsoft Edge: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 27 Oct 2023

**[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 27 Oct 2023

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

Ein entfernter Angreifer kann mehrere Schwachstellen in F5 BIG-IP ausnutzen, um Sicherheitsmaßnahmen zu umgehen und beliebigen Code auszuführen.

- [Link](#)

---

Fri, 27 Oct 2023

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

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um beliebigen Programmcode auszuführen, um Informationen offenzulegen und um Anfragen zu manipulieren.

- [Link](#)

---

Fri, 27 Oct 2023

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

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 27 Oct 2023

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

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

---

Fri, 27 Oct 2023

**[UPDATE] [hoch] IBM Operational Decision Manager: Mehrere Schwachstellen**

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in IBM Operational Decision Manager ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- [Link](#)

---

Fri, 27 Oct 2023

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung**

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/30/2023	[GLSA-202310-20 : rxvt-unicode: Arbitrary Code Execution]	critical
10/30/2023	[GLSA-202310-18 : Rack: Multiple Vulnerabilities]	critical
10/30/2023	[Ubuntu 22.04 LTS : Node.js vulnerabilities (USN-6457-1)]	critical
10/30/2023	[Ubuntu 20.04 ESM / 22.04 ESM : Slurm vulnerabilities (USN-6458-1)]	critical
10/30/2023	[GLSA-202310-19 : Dovecot: Privilege Escalation]	high
10/30/2023	[CBL Mariner 2.0 Security Update: vim (CVE-2023-5344)]	high
10/30/2023	[RHEL 9 : libguestfs-winsupport (RHSA-2023:6168)]	high
10/30/2023	[RHEL 9 : libguestfs-winsupport (RHSA-2023:6167)]	high
10/30/2023	[RHEL 7 : firefox (RHSA-2023:6162)]	high
10/30/2023	[Debian DLA-3640-1 : distro-info - LTS test-suite update]	high
10/30/2023	[Debian DLA-3639-1 : distro-info-data - LTS database update]	high
10/30/2023	[Ubuntu 23.10 : Linux kernel vulnerabilities (USN-6454-2)]	high
10/30/2023	[Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6441-3)]	high
10/30/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : vorbis-tools (SUSE-SU-2023:4251-1)]	high
10/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 34 for SLE 15 SP3) (SUSE-SU-2023:4239-1)]	high
10/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 36 for SLE 15 SP3) (SUSE-SU-2023:4261-1)]	high
10/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 40 for SLE 15 SP2) (SUSE-SU-2023:4243-1)]	high
10/30/2023	[SUSE SLES12 Security Update : nodejs12 (SUSE-SU-2023:4259-1)]	high
10/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 38 for SLE 15 SP2) (SUSE-SU-2023:4245-1)]	high
10/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 35 for SLE 15 SP3) (SUSE-SU-2023:4260-1)]	high
10/30/2023	[SUSE SLES15 Security Update : kernel (Live Patch 37 for SLE 15 SP3) (SUSE-SU-2023:4264-1)]	high
10/30/2023	[SUSE SLES12 / SLES15 Security Update : kernel (Live Patch 35 for SLE 15 SP1) (SUSE-SU-2023:4244-1)]	high
10/30/2023	[AlmaLinux 9 : libguestfs-winsupport (ALSA-2023:6167)]	high
10/30/2023	[RHEL 8 : thunderbird (RHSA-2023:6198)]	high
10/30/2023	[RHEL 8 : firefox (RHSA-2023:6185)]	high
10/30/2023	[RHEL 8 : firefox (RHSA-2023:6187)]	high
10/30/2023	[RHEL 8 : firefox (RHSA-2023:6186)]	high
10/30/2023	[RHEL 9 : thunderbird (RHSA-2023:6192)]	high
10/30/2023	[RHEL 8 : thunderbird (RHSA-2023:6196)]	high
10/30/2023	[RHEL 8 : firefox (RHSA-2023:6190)]	high
10/30/2023	[RHEL 8 : thunderbird (RHSA-2023:6194)]	high
10/30/2023	[RHEL 8 : thunderbird (RHSA-2023:6197)]	high
10/30/2023	[RHEL 9 : firefox (RHSA-2023:6199)]	high
10/30/2023	[RHEL 9 : firefox (RHSA-2023:6188)]	high
10/30/2023	[RHEL 9 : thunderbird (RHSA-2023:6191)]	high
10/30/2023	[RHEL 8 : firefox (RHSA-2023:6189)]	high
10/30/2023	[RHEL 8 : thunderbird (RHSA-2023:6195)]	high
10/30/2023	[Fedora 38 : rt (2023-64fe19f832)]	high
10/30/2023	[Fedora 38 : thunderbird (2023-126cfa741)]	high
10/30/2023	[Fedora 37 : slurm (2023-1f851fa869)]	high
10/30/2023	[Fedora 38 : slurm (2023-234df8a1d4)]	high
10/30/2023	[Amazon Linux 2023 : squid (ALAS2023-2023-402)]	high
10/30/2023	[Oracle Linux 9 : libguestfs-winsupport (ELSA-2023-6167)]	high
10/30/2023	[Oracle Linux 7 : firefox (ELSA-2023-6162)]	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

## Die Hacks der Woche

mit Martin Haunschmid

Über 60.000 Unternehmen mit 1 Lücke gehackt. WHAT. Cisco, Okta



[Zum Youtube Video](#)

## Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2023-10-30	Südwestfalen-IT	[DEU]	<a href="#">Link</a>
2023-10-28	Bibliothèque publique de Toronto	[CAN]	<a href="#">Link</a>
2023-10-28	Designa Verkehrsleittechnik	[DEU]	<a href="#">Link</a>
2023-10-27	Vinovalie	[FRA]	<a href="#">Link</a>
2023-10-26	Annecy	[FRA]	<a href="#">Link</a>
2023-10-25	Michael Garron Hospital	[CAN]	<a href="#">Link</a>
2023-10-23	Hôpital de Vérone	[ITA]	<a href="#">Link</a>
2023-10-23	L'EHPAD "Les Hortensias" à Marigny-le-Lozon	[FRA]	<a href="#">Link</a>
2023-10-23	Grupo GTD	[CHL]	<a href="#">Link</a>
2023-10-23	Allen Park Public Schools	[USA]	<a href="#">Link</a>
2023-10-22	TransForm	[CAN]	<a href="#">Link</a>
2023-10-22	La Prefeitura de Araguari	[BRA]	<a href="#">Link</a>
2023-10-21	Comté de Clark	[USA]	<a href="#">Link</a>
2023-10-20	Museum d'Histoire Naturelle de Berlin	[DEU]	<a href="#">Link</a>
2023-10-20	Le bureau du procureur du comté d'Orange	[USA]	<a href="#">Link</a>
2023-10-19	Glynn County	[USA]	<a href="#">Link</a>
2023-10-19	Cabo Verde Telecom	[CPV]	<a href="#">Link</a>
2023-10-19	WESTbahn	[AUT]	<a href="#">Link</a>
2023-10-19	Clinique Deegenberg	[DEU]	<a href="#">Link</a>
2023-10-17	La Real Sociedad	[ESP]	<a href="#">Link</a>
2023-10-17	Everi	[USA]	<a href="#">Link</a>
2023-10-17	Hopewell Area School District	[USA]	<a href="#">Link</a>
2023-10-17	Logan Systems Inc.	[USA]	<a href="#">Link</a>
2023-10-16	Psychiatrie Baselland	[CHE]	<a href="#">Link</a>
2023-10-16	Patriotisk Selskab	[DNK]	<a href="#">Link</a>
2023-10-16	Hong Kong Ballet	[HKG]	<a href="#">Link</a>
2023-10-16	La Provincia di Perugia	[ITA]	<a href="#">Link</a>
2023-10-16	Harlingen Police Department	[USA]	<a href="#">Link</a>
2023-10-15	Système judiciaire du Kansas	[USA]	<a href="#">Link</a>
2023-10-15	WMCHHealth hospital	[USA]	<a href="#">Link</a>
2023-10-15	Westchester Medical Center	[USA]	<a href="#">Link</a>
2023-10-15	American Family Insurance	[USA]	<a href="#">Link</a>
2023-10-14	Henry Schein Inc.	[USA]	<a href="#">Link</a>
2023-10-12	Service Départemental d'Incendie et de Secours des Pyrénées-Atlantiques (SDIS64)	[FRA]	<a href="#">Link</a>
2023-10-12	Verhelst	[BEL]	<a href="#">Link</a>
2023-10-11	Akumin	[USA]	<a href="#">Link</a>
2023-10-10	Simpson Manufacturing Co.	[USA]	<a href="#">Link</a>
2023-10-10	Pride of Nottingham (PON)	[GBR]	<a href="#">Link</a>
2023-10-10	Le Cofrac	[FRA]	<a href="#">Link</a>
2023-10-09	De La Salle University (DLSU)	[PHL]	<a href="#">Link</a>
2023-10-09	Kwik Trip	[USA]	<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>
2023-10-05	Clark County School District (CCSD)	[USA]	<a href="#">Link</a>
2023-10-04	Hochsauerlandenergie et Hochsauerlandwasser	[DEU]	<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
2023-10-31	[Kinesis Film Srl]	knight	<a href="#">Link</a>
2023-10-31	[BMW Munique Motors]	knight	<a href="#">Link</a>
2023-10-31	[Benefit Management]	knight	<a href="#">Link</a>
2023-10-31	[Intellipop Fiber Internet]	knight	<a href="#">Link</a>
2023-10-31	[il Centro]	knight	<a href="#">Link</a>
2023-10-31	[Emmea Srl]	knight	<a href="#">Link</a>
2023-10-31	[Michels Markisen GmbH]	knight	<a href="#">Link</a>
2023-10-31	[Pontifica Universidad Católica de Chile]	knight	<a href="#">Link</a>
2023-10-31	[Veneto Transportes]	knight	<a href="#">Link</a>
2023-10-30	[Brodart]	play	<a href="#">Link</a>
2023-10-30	[ecabusinessenergy.com]	lockbit3	<a href="#">Link</a>
2023-10-30	[frontlineequipment.com.au]	lockbit3	<a href="#">Link</a>
2023-10-30	[groupemontclair.com]	lockbit3	<a href="#">Link</a>
2023-10-30	[aces-int.com]	lockbit3	<a href="#">Link</a>
2023-10-30	[aiq.com.mx]	lockbit3	<a href="#">Link</a>
2023-10-30	[Freeman Johnson]	akira	<a href="#">Link</a>
2023-10-30	[RANSOMEDVC is for sale]	ransomed	<a href="#">Link</a>
2023-10-30	[Jockey Club]	medusa	<a href="#">Link</a>
2023-10-30	[topcharoen.co.th]	lockbit3	<a href="#">Link</a>
2023-10-30	[mottamaholdings.com]	lockbit3	<a href="#">Link</a>
2023-10-29	[Global Export Marketing Co. Ltd.]	incransom	<a href="#">Link</a>
2023-10-29	[WACOSA]	alphv	<a href="#">Link</a>
2023-10-28	[IBACOS]	8base	<a href="#">Link</a>
2023-10-28	[Dallas County]	play	<a href="#">Link</a>
2023-10-28	[Alpha Mortgage]	play	<a href="#">Link</a>
2023-10-28	[Encompass Elements]	play	<a href="#">Link</a>
2023-10-28	[CK Associates]	play	<a href="#">Link</a>
2023-10-28	[Yingling Aviation]	play	<a href="#">Link</a>
2023-10-28	[Sam Tell Companies]	play	<a href="#">Link</a>
2023-10-28	[Waterstone Faucets]	play	<a href="#">Link</a>
2023-10-28	[Bush Refrigeration]	play	<a href="#">Link</a>
2023-10-28	[Drug Emporium]	play	<a href="#">Link</a>
2023-10-28	[Online Development]	play	<a href="#">Link</a>
2023-10-28	[KDI Office Technology]	play	<a href="#">Link</a>
2023-10-28	[Het Veer]	play	<a href="#">Link</a>
2023-10-28	[TNT Plastic Molding]	bianlian	<a href="#">Link</a>
2023-10-28	[Morrison Community Hospital FULL HUGE LEAK + BONUS]	alphv	<a href="#">Link</a>
2023-10-28	[ISRAEL STOP GENOCIDE IN GAZA]	alphv	<a href="#">Link</a>
2023-10-27	[boeing.com]	lockbit3	<a href="#">Link</a>
2023-10-27	[Alam Flora Sdn Bhd]	incransom	<a href="#">Link</a>
2023-10-27	[Telecommunications Services of Trinidad and Tobago (tsstt.co.tt)]	ransomexx	<a href="#">Link</a>
2023-10-27	[tilden-coil.com]	lockbit3	<a href="#">Link</a>
2023-10-27	[Mutual Underwriters]	alphv	<a href="#">Link</a>
2023-10-27	[Stanford University]	akira	<a href="#">Link</a>
2023-10-27	[VOLEX.COM]	blackbasta	<a href="#">Link</a>
2023-10-27	[Wilson Lewis]	8base	<a href="#">Link</a>
2023-10-27	[ZINSER GmbH]	8base	<a href="#">Link</a>
2023-10-27	[CBS]	alphv	<a href="#">Link</a>
2023-10-26	[maniland.co.uk]	threeam	<a href="#">Link</a>
2023-10-20	[Laiho Group]	play	<a href="#">Link</a>
2023-10-26	[caminorealcs.org]	lockbit3	<a href="#">Link</a>
2023-10-26	[doverchem.com]	lockbit3	<a href="#">Link</a>
2023-10-26	[SG World]	qilin	<a href="#">Link</a>
2023-10-26	[claimtek.com]	threeam	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-26	[apexga.bank]	abyss	Link
2023-10-26	[Versatile Card Technology Private Limited]	mallox	Link
2023-10-25	[Fortive Corporation]	blackbasta	Link
2023-10-25	[M&n Management]	snatch	Link
2023-10-25	[Ancillae-Assumpta Academy]	snatch	Link
2023-10-25	[Direct Mail Corporation]	incransom	Link
2023-10-25	[Carter Transport Claims]	8base	Link
2023-10-25	[AVA Limited]	8base	Link
2023-10-25	[Pine River Pre-Pack, Inc]	8base	Link
2023-10-25	[Harmann Studios Inc]	8base	Link
2023-10-15	[Broad River Retail/Ashley Store]	lorenz	Link
2023-10-25	[Paul-Alexandre Doïcesco, Notaires Associés]	qilin	Link
2023-10-25	[Cardiovascular Consultants Ltd]	qilin	Link
2023-10-25	[LBA]	alphv	Link
2023-10-24	[camico.com]	lockbit3	Link
2023-10-24	[excon.cl]	lockbit3	Link
2023-10-24	[martinsonservices.com]	lockbit3	Link
2023-10-23	[Florists Supply Ltd]	noescape	Link
2023-10-23	[City of Victorville]	noescape	Link
2023-10-24	[fern-plastics.co.uk]	lockbit3	Link
2023-10-24	[ambic.co.uk]	lockbit3	Link
2023-10-24	[mgbwlaw.com]	lockbit3	Link
2023-10-24	[linkmicrotek.com]	lockbit3	Link
2023-10-24	[CMC Group]	akira	Link
2023-10-24	[City of Pittsburg]	alphv	Link
2023-10-24	[EDUARDO G. BARROSO]	8base	Link
2023-10-24	[grupocobra.com]	lockbit3	Link
2023-10-24	[SURTECO North America]	8base	Link
2023-10-23	[3-D Engineering/ 3-D Precision Machine]	alphv	Link
2023-10-23	[www.portage.k12.in.us]	alphv	Link
2023-10-23	[Newconcepttech]	cuba	Link
2023-10-23	[University of Defence - Full Leak]	monti	Link
2023-10-23	[Penfield Fire Company]	noescape	Link
2023-10-23	[Korea Petroleum Industries Company]	noescape	Link
2023-10-23	[Gasmart Organization]	noescape	Link
2023-10-23	[KBS Accountants, Tax Specialists & Lawyers]	noescape	Link
2023-10-23	[INSTANT ACCESS]	noescape	Link
2023-10-23	[Misterminit]	noescape	Link
2023-10-23	[Central University of Bayamón]	noescape	Link
2023-10-23	[Motorcycles of Charlotte & Greensboro]	noescape	Link
2023-10-23	[International Community Schools]	noescape	Link
2023-10-23	[Order of Psychologists of Lombardy]	noescape	Link
2023-10-23	[Panificio Grandolfo]	blackbasta	Link
2023-10-23	[3-D Engineering]	alphv	Link
2023-10-23	[Safpro]	medusa	Link
2023-10-23	[EHPAD]	medusa	Link
2023-10-23	[Beaver Lake Cree Nation]	medusa	Link
2023-10-23	[Native Counselling Services of Alberta]	medusa	Link
2023-10-23	[Ada-Borup-West School]	medusalocker	Link
2023-10-23	[wellons.org]	medusalocker	Link
2023-10-23	[harlingentx.gov]	lockbit3	Link
2023-10-23	[mamu.be]	lockbit3	Link
2023-10-22	[Ransomedvc Launches A forum]	ransomed	Link
2023-10-22	[Dr. Jaime Schwartz MD, FACS]	hunters	Link
2023-10-22	[Edwards Business Systems]	8base	Link
2023-10-22	[Brunton Shaw]	8base	Link
2023-10-22	[JC Roman Construction]	8base	Link
2023-10-22	[APS - Automotive Parts Solutions]	8base	Link
2023-10-21	[chs.ca]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-21	[Panetteria Grandolfo]	blackbasta	<a href="#">Link</a>
2023-10-21	[Simpson Strong-Tie]	blackbasta	<a href="#">Link</a>
2023-10-21	[Sidockgroup.]	donutleaks	<a href="#">Link</a>
2023-10-21	[The Law Offices of Julian Lewis Sanders & Associates FULL LEAK!]	alphv	<a href="#">Link</a>
2023-10-20	[Williamson Foodservice]	play	<a href="#">Link</a>
2023-10-20	[Epaccsys]	play	<a href="#">Link</a>
2023-10-20	[Tru-val Electric]	play	<a href="#">Link</a>
2023-10-20	[Bridgeport Fittings]	play	<a href="#">Link</a>
2023-10-20	[Kobi Karp Architecture and Interior Design]	play	<a href="#">Link</a>
2023-10-20	[RADISE]	play	<a href="#">Link</a>
2023-10-20	[Polar Tech Industries]	play	<a href="#">Link</a>
2023-10-20	[Ipswich Bay Glass]	play	<a href="#">Link</a>
2023-10-20	[Hygieneering]	play	<a href="#">Link</a>
2023-10-20	[The Fountain Group]	play	<a href="#">Link</a>
2023-10-20	[Venture Plastics]	play	<a href="#">Link</a>
2023-10-20	[Milk Source]	play	<a href="#">Link</a>
2023-10-20	[We Hire Pentesters(5BTC Payout)]	ransomed	<a href="#">Link</a>
2023-10-20	[uaes.com]	lockbit3	<a href="#">Link</a>
2023-10-20	[degrootgroep.nl]	lockbit3	<a href="#">Link</a>
2023-10-20	[charleystaxi.com]	lockbit3	<a href="#">Link</a>
2023-10-12	[UK Stratton Primary School]	hunters	<a href="#">Link</a>
2023-10-20	[Royal College of Physicians and Surgeons of Glasgow]	akira	<a href="#">Link</a>
2023-10-20	[Southland Integrated Services]	akira	<a href="#">Link</a>
2023-10-20	[Protector Fire Services]	akira	<a href="#">Link</a>
2023-10-20	[kvc constructors inc]	alphv	<a href="#">Link</a>
2023-10-19	[Superline - Full Leak]	monti	<a href="#">Link</a>
2023-10-19	[Government of Brazil - Business Information Brazil]	blacksuit	<a href="#">Link</a>
2023-10-19	[Associated Wholesale Grocers]	play	<a href="#">Link</a>
2023-10-19	[Visionary Integration Professionals]	akira	<a href="#">Link</a>
2023-10-19	[Inventum Øst]	akira	<a href="#">Link</a>
2023-10-19	[nirolaw.com]	lockbit3	<a href="#">Link</a>
2023-10-19	[QuadraNet Enterprises]	akira	<a href="#">Link</a>
2023-10-19	[hgmonline.com]	lockbit3	<a href="#">Link</a>
2023-10-19	[salaw.com]	lockbit3	<a href="#">Link</a>
2023-10-19	[frs-fnrs.be]	lockbit3	<a href="#">Link</a>
2023-10-19	[thecsi.com]	lockbit3	<a href="#">Link</a>
2023-10-19	[smart-union.org]	lockbit3	<a href="#">Link</a>
2023-10-19	[Innovattel LLC]	alphv	<a href="#">Link</a>
2023-10-19	[CADRE]	alphv	<a href="#">Link</a>
2023-10-18	[fdf.org]	lockbit3	<a href="#">Link</a>
2023-10-18	[Dow Golub Remels & Gilbreath]	bianlian	<a href="#">Link</a>
2023-10-18	[Griffing & Company, P.C]	bianlian	<a href="#">Link</a>
2023-10-18	[International Biomedical Ltd]	bianlian	<a href="#">Link</a>
2023-10-18	[Jebsen & Co. Ltd.]	bianlian	<a href="#">Link</a>
2023-10-12	[KBS Accountants]	noescape	<a href="#">Link</a>
2023-10-17	[Rotorcraft Leasing Company]	0mega	<a href="#">Link</a>
2023-10-17	[Catarineau & Givens P.A. FULL LEAK!]	alphv	<a href="#">Link</a>
2023-10-17	[kasperekusaoptical.com]	lockbit3	<a href="#">Link</a>
2023-10-17	[SIIX Corporation]	alphv	<a href="#">Link</a>
2023-10-17	[STANTON WILLIAMS]	blackbasta	<a href="#">Link</a>
2023-10-17	[Edwardian Hotels London]	blackbasta	<a href="#">Link</a>
2023-10-17	[HAFFNER GmbH Co.]	blackbasta	<a href="#">Link</a>
2023-10-17	[Intred]	blackbasta	<a href="#">Link</a>
2023-10-17	[Ampersand]	blackbasta	<a href="#">Link</a>
2023-10-17	[BACCARAT]	blackbasta	<a href="#">Link</a>
2023-10-17	[PIEMME S.p.A.]	blackbasta	<a href="#">Link</a>
2023-10-17	[Greenpoint]	incransom	<a href="#">Link</a>
2023-10-09	[Gasmart]	noescape	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-16	[cpstate.org]	lockbit3	Link
2023-10-16	[ATI Traduction]	medusa	Link
2023-10-16	[EDB ]	medusa	Link
2023-10-16	[Global Product Sales]	medusa	Link
2023-10-16	[Symposia Organizzazione Congressi S.R.L]	medusa	Link
2023-10-16	[sdproducts.co.uk]	lockbit3	Link
2023-10-16	[SCS SpA]	cactus	Link
2023-10-16	[OmniVision Technologies]	cactus	Link
2023-10-16	[Believe Productions]	medusa	Link
2023-10-16	[Ransomedvc Pentest Services!]	ransomed	Link
2023-10-09	[Mount Holly Nissan]	noescape	Link
2023-10-16	[Boise Rescue Mission Ministries]	alphv	Link
2023-10-16	[DOMAIN-BACCARAT_2]	blackbasta	Link
2023-10-16	[NCC_2]	blackbasta	Link
2023-10-16	[RE : Clarification]	ransomed	Link
2023-10-16	[Rob Lee Evidence : Sneak Peek]	ransomed	Link
2023-10-16	[Cogal Industry]	snatch	Link
2023-10-15	[Islamic Azad University Electronic Campus]	arvinclub	Link
2023-10-15	[Colonial Pipeline Company]	ransomed	Link
2023-10-15	[Accenture Breach Evidence & Debunking Rob Lee's Lies]	ransomed	Link
2023-10-15	[webpag.com.br database leaked]	ransomed	Link
2023-10-15	[QSI INC - Credit Cards & Transaction Processing]	alphv	Link
2023-10-14	[DUHOCAAU]	mallox	Link
2023-10-14	[The Law Offices of Julian Lewis Sanders & Associates]	alphv	Link
2023-10-14	[Jahesh Innovation]	arvinclub	Link
2023-10-14	[Northwest Eye Care Professionals]	rhysida	Link
2023-10-14	[Intech]	snatch	Link
2023-10-13	[Catholic Charities]	incransom	Link
2023-10-13	[Kimia Tadbir Kiyan]	arvinclub	Link
2023-10-05	[Korea Petroleum Industrial Co. Ltd]	noescape	Link
2023-10-13	[Cleveland City Schools]	incransom	Link
2023-10-13	[Alconex Specialty Products]	trigona	Link
2023-10-13	[Multidev Technologies]	blacksuit	Link
2023-10-13	[Morrison Community Hospital]	alphv	Link
2023-10-13	[Hospital Italiano de Buenos Aires]	knight	Link
2023-10-13	[AKBASOGLU HOLDING Trans KA]	knight	Link
2023-10-13	[Metroclub.org]	ransomed	Link
2023-10-13	[Optimity UK]	ransomed	Link
2023-10-13	[Baumit Bulgaria]	ransomed	Link
2023-10-13	[novoingresso.com.br]	ransomed	Link
2023-10-13	[webpag.com.br]	ransomed	Link
2023-10-13	[rodoviariaonline.com.br]	ransomed	Link
2023-10-13	[Kasida.bg Database Leaked, Download]	ransomed	Link
2023-10-13	[I&G Brokers Database, Download Now]	ransomed	Link
2023-10-13	[pilini.bg Database, Download Now!]	ransomed	Link
2023-10-13	[iLife.bg]	ransomed	Link
2023-10-13	[Fuck Palestine! We buy your access!!]	ransomed	Link
2023-10-13	[NEW TWITTER]	ransomed	Link
2023-10-12	[Vicon industries inc.]	incransom	Link
2023-10-05	[Seattle Housing Authority]	noescape	Link
2023-10-12	[FPZ]	trigona	Link
2023-10-12	[Tri-Way Manufacturing Technologies]	moneymessage	Link
2023-10-12	[Neodata]	medusa	Link
2023-10-12	[Evasión ]	medusa	Link
2023-10-12	[SIMTA ]	medusa	Link
2023-10-12	[ZOUARY & Associés ]	medusa	Link
2023-10-10	[Comtek Advanced Structures, a Latecoere Company]	8base	Link



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-10-10	[KTUA Landscape Architecture and Planning]	8base	<a href="#">Link</a>
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>
2023-10-08	[urc-automation.com]	lockbit3	<a href="#">Link</a>
2023-10-08	[IKM]	alphv	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[pico soft.biz]	lockbit3	Link
2023-10-06	[litung.com.tw]	lockbit3	Link
2023-10-05	[Granger Medical Clinic]	noescape	Link
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	Link
2023-10-04	[suncoast-chc.org]	lockbit3	Link
2023-10-04	[Meridian Cooperative]	blackbyte	Link
2023-10-04	[Roof Management]	play	Link
2023-10-04	[Security Instrument]	play	Link
2023-10-04	[Filtration Control]	play	Link
2023-10-04	[Cinapolis USA]	play	Link
2023-10-04	[CHARMANT Group]	play	Link
2023-10-04	[Stavanger Municipality]	play	Link
2023-10-04	[Gruskin Group]	akira	Link
2023-10-04	[McLaren Health Care Corporation]	alphv	Link
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	Link
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	Link
2023-10-02	[Confidential files]	medusalocker	Link
2023-10-02	[Pain Care]	alphv	Link
2023-10-02	[Windak]	medusa	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
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.