Cybersecurity Morgenreport

Ausgabe: 20231005

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: Attacken auf Android 11, 12 und 13 beobachtet
Unter anderem Google hat wichtige Sicherheitsupdates für Android-Geräte veröffentlicht. Zwei Lücken haben Angreifer bereits im Visier.
- Link

—

Webbrowser: Update für Google Chrome schließt Lücke mit hohem Risiko
Google hat dem Webbrowser Chrome ein Sicherheitsupdate spendiert. Es schließt eine Lücke mit hohem Bedrohungsgrad.
- Link

—

Angriffe auf ältere Android-Geräte: Lücke in Mali-GPU nur teilweise geschlossen
Aufgrund mehrerer Schwachstellen im Treiber der Grafikeinheit Mali sind unter anderem Smartphone-Modelle von Samsung und Xiaomi verwundbar.
- Link

—

Erste Angriffe gesichtet: Angreifer können über Lücken in WS_FTP Daten löschen
Das Softwarepaket für Dateiübertragung WS_FTP ist verwundbar. Die Entwickler haben mehrere Sicherheitslücken geschlossen. Mittlerweile gibt es erste Attacken.
- Link

—

Jetzt patchen! Ransomware schlüpft durch kritische TeamCity-Lücke
Angreifer nutzen eine Sicherheitslücke des Software-Distributionssystems TeamCity aus, das weltweit über 30.000 Firmen wie Citibank, HP und Nike einsetzen.
- Link

—

Jetzt patchen! Exploit für kritische Sharepoint-Lücke veröffentlicht
Admins sollten ihre Sharepoint-Server zügig patchen, denn für eine im Juni durch Microsoft behobene Lücke steht jetzt ein Proof-of-Concept-Exploit bereit.
- Link

—

Kritische Lücke im Mailserver Exim
Der SMTP-Dienst des freien Mailservers Exim enthält eine kritische Schwachstelle, über die Angreifer beliebigen Code ausführen können. Updates sind unterwegs.
- Link

—

Jetzt patchen! Angreifer haben Netzwerkgeräte von Cisco im Visier
Cisco hat unter anderem eine kritische Lücke in Catalyst SD-WAN geschlossen. Außerdem gibt es Sicherheitsupdates für weitere Produkte.
- Link

—

Unzählige Anwendungen betroffen: Chaos bei WebP-Lücke
Eine Sicherheitslücke im WebP-Grafikformat betrifft über Googles Chrome hinaus deutlich mehr Anwendungen.
- Link

—

Zehn Sicherheitslücken in Chrome geschlossen, eine wird bereits ausgenutzt
Google sichert seinen Webbrowser Chrome abermals gegen laufende Attacken 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-2023-38035	0.970820000	0.996860000	Link
CVE-2023-35078	0.955330000	0.991670000	Link
CVE-2023-34362	0.920100000	0.985980000	Link
CVE-2023-33246	0.971460000	0.997180000	Link
CVE-2023-32315	0.960720000	0.992970000	Link
CVE-2023-30625	0.932650000	0.987620000	Link
CVE-2023-28771	0.926550000	0.986800000	Link
CVE-2023-27524	0.936870000	0.988200000	Link
CVE-2023-27372	0.971740000	0.997360000	Link
CVE-2023-27350	0.971370000	0.997120000	Link
CVE-2023-26469	0.918080000	0.985800000	Link
CVE-2023-26360	0.915880000	0.985560000	Link
CVE-2023-25717	0.961530000	0.993160000	Link
CVE-2023-25194	0.924830000	0.986560000	Link
CVE-2023-2479	0.963650000	0.993860000	Link
CVE-2023-24489	0.967770000	0.995470000	Link
CVE-2023-21839	0.951010000	0.990640000	Link
CVE-2023-21823	0.929300000	0.987150000	Link
CVE-2023-21554	0.961360000	0.993130000	Link
CVE-2023-20887	0.944590000	0.989420000	Link
CVE-2023-0669	0.967330000	0.995320000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 04 Oct 2023
[UPDATE] [kritisch] JetBrains TeamCity: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in JetBrains TeamCity ausnutzen, um beliebigen Programmcode auszuführen oder einen Cross Site Scripting Angriff durchzuführen.
- Link

—

Wed, 04 Oct 2023
[UPDATE] [hoch] Progress Software WS_FTP: Mehre Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Progress Software WS_FTP ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder Cross-Site Scripting und Cross-Site Request Forgery Angriffe durchzuführen.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

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

- Link

—

Wed, 04 Oct 2023

[NEU] [hoch] Google Android: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Wed, 04 Oct 2023

[NEU] [hoch] PyTorch: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PyTorch ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 04 Oct 2023

[NEU] [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, 04 Oct 2023

[NEU] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 04 Oct 2023

[NEU] [hoch] Samsung Android: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und seine Rechte zu erweitern.

- Link

—

Wed, 04 Oct 2023

[NEU] [hoch] Mattermost: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Mattermost ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Red Hat rh-nodejs8-nodejs: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat rh-nodejs8-nodejs ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Nvidia Treibern ausnutzen, um seine Privilegien zu erhöhen, einen Denial of Service Angriff durchzuführen, vertrauliche Daten einzusehen, Daten zu manipulieren oder die Integrität zu gefährden.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Nvidia Treiber ausnutzen, um beliebigen Code auszuführen, einen Denial of Service Zustand zu verursachen, vertrauliche Informationen offenzulegen und Daten zu manipulieren.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Erlangen von Administratorrechten

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um Administratorrechte zu erlangen.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Offenlegung von Informationen

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um Informationen offenzulegen.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

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

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Nvidia Treiber: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Nvidia Treiber ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Grafana: Mehrere Schwachstellen

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

- Link

—

Wed, 04 Oct 2023

[UPDATE] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode auszuführen, ein Cross-Site-Scritping-Angriff durchzuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/4/2023	[Sophos Intercept X Detection and Status]	critical
10/4/2023	[Apache Spark < 3.4.0 Privilege Escalation (CVE-2023-22946)]	critical
10/4/2023	[Oracle Linux 9 : nodejs (ELSA-2023-5363)]	critical
10/4/2023	[Ubuntu 20.04 LTS / 22.04 LTS : FreeRDP vulnerabilities (USN-6401-1)]	critical
10/4/2023	[Cisco Adaptive Security Appliance Software Remote Access VPN Unauthorized Access - Brute Force Attack (cisco-sa-asaftd-ravpn-auth-8LyfCkeC)]	critical
10/4/2023	[Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Exim vulnerabilities (USN-6411-1)]	critical
10/4/2023	[Ubuntu 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6412-1)]	critical
10/4/2023	[RHEL 8 : firefox (RHSA-2023:5440)]	critical
10/4/2023	[RHEL 9 : thunderbird (RHSA-2023:5435)]	critical
10/4/2023	[RHEL 8 : firefox (RHSA-2023:5433)]	critical
10/4/2023	[RHEL 8 : thunderbird (RHSA-2023:5429)]	critical
10/4/2023	[RHEL 9 : firefox (RHSA-2023:5427)]	critical
10/4/2023	[RHEL 8 : thunderbird (RHSA-2023:5428)]	critical
10/4/2023	[RHEL 9 : firefox (RHSA-2023:5434)]	critical
10/4/2023	[RHEL 8 : firefox (RHSA-2023:5436)]	critical
10/4/2023	[RHEL 9 : thunderbird (RHSA-2023:5439)]	critical
10/4/2023	[RHEL 8 : firefox (RHSA-2023:5426)]	critical
10/4/2023	[RHEL 8 : firefox (RHSA-2023:5437)]	critical
10/4/2023	[RHEL 8 : thunderbird (RHSA-2023:5430)]	critical
10/4/2023	[RHEL 8 : thunderbird (RHSA-2023:5432)]	critical
10/4/2023	[RHEL 8 : thunderbird (RHSA-2023:5438)]	critical
10/4/2023	[Ubuntu 22.04 LTS : Linux kernel (OEM) vulnerabilities (USN-6415-1)]	critical
10/4/2023	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-6416-1)]	critical
10/4/2023	[FreeBSD : libspf2 – Integer Underflow Remote Code Execution (915855ad-283d-4597-b01e-e0bf611db78b)]	critical
10/4/2023	[QEMU < 8.1.1 Multiple Vulnerabilities]	high
10/4/2023	[FreeBSD : chromium – type confusion in v8 (4e45c45b-629e-11ee-8290-a8a1599412c6)]	high
10/4/2023	[GLSA-202310-04 : libvpx: Multiple Vulnerabilities]	high
10/4/2023	[Progress WS_FTP Server < 8.7.4, 8.8.0 < 8.8.2 Multiple Vulnerabilities]	high
10/4/2023	[Wireshark 3.6.x < 3.6.17 A Vulnerability]	high
10/4/2023	[Wireshark 3.6.x < 3.6.17 A Vulnerability (macOS)]	high
10/4/2023	[Wireshark 4.0.x < 4.0.9 A Vulnerability]	high
10/4/2023	[Wireshark 4.0.x < 4.0.9 A Vulnerability (macOS)]	high
10/4/2023	[Ubuntu 20.04 LTS : Django vulnerability (USN-6414-1)]	high
10/4/2023	[Ubuntu 16.04 ESM : GNU binutils vulnerabilities (USN-6413-1)]	high
10/4/2023	[Fedora 38 : pgadmin4 (2023-8cc61c8b14)]	high
10/4/2023	[Fedora 38 : drupal7 (2023-f4d22f8a92)]	high
10/4/2023	[Fedora 38 : golang-github-cncf-xds / golang-github-envoyproxy-control-plane / etc (2023-f122ea1b3e)]	high
10/4/2023	[Fedora 37 : drupal7 (2023-83aeb73043)]	high
10/4/2023	[Fedora 37 : pgadmin4 (2023-478aa17fa2)]	high
10/4/2023	[Atlassian Confluence 8.x < 8.3.3 / 8.4.x < 8.4.3 / 8.5.x < 8.5.2 (CONFSERVER-92475)]	high
10/4/2023	[Microsoft Edge (Chromium) < 117.0.2045.55 (CVE-2023-5346)]	high
10/4/2023	[Debian DSA-5515-1 : chromium - security update]	high

Aktiv ausgenutzte Sicherheitslücken

Exploits

“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
—
” “Tue, 03 Oct 2023
SAP Enable Now Manager 10.6.5 Build 2804 Cloud Edition CSRF / XSS / Redirect
SAP Enable Now Manager version 10.6.5 Build 2804 Cloud Edition suffers from cross site request forgery, cross site scripting, and open redirection vulnerabilities.
- Link
—
” “Tue, 03 Oct 2023
openVIVA c2 20220101 Cross Site Scripting
openVIVA c2 suffers from a persistent cross site scripting vulnerability. Versions prior to 20220801 are affected.
- Link
—
” “Tue, 03 Oct 2023
WordPress Contact Form Generator 2.5.5 Cross Site Scripting
WordPress Contact Form Generator plugin version 2.5.5 suffers from a cross site scripting vulnerability.
- Link
—
” “Tue, 03 Oct 2023
WordPress KiviCare 3.2.0 Cross Site Scripting
WordPress KiviCard plugin version 3.2.0 suffers from a cross site scripting vulnerability.
- Link
—
” “Mon, 02 Oct 2023
Packet Storm New Exploits For September, 2023
This archive contains all of the 122 exploits added to Packet Storm in September, 2023.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter Pre-Auth MPFS Image Remote Code Execution
Electrolink FM/DAB/TV Transmitter allows access to an unprotected endpoint that allows an MPFS File System binary image upload without authentication. The MPFS2 file system module provides a light-weight read-only file system that can be stored in external EEPROM, external serial Flash, or internal Flash program memory. This file system serves as the basis for the HTTP2 web server module, but is also used by the SNMP module and is available to other applications that require basic read-only storage capabilities. This can be exploited to overwrite the flash program memory that holds the web server’s main interfaces and execute arbitrary code.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter Unauthenticated Remote Denial Of Service
Electrolink FM/DAB/TV Transmitter from a denial of service scenario. An unauthenticated attacker can reset the board as well as stop the transmitter operations by sending one GET request to the command.cgi gateway.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter SuperAdmin Hidden Functionality
Electrolink FM/DAB/TV Transmitter allows an unauthenticated attacker to bypass authentication and modify the Cookie to reveal hidden pages that allows more critical operations to the transmitter.
- Link
—

” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter Vertical Privilege Escalation
Electrolink FM/DAB/TV Transmitter suffers from a privilege escalation vulnerability. An attacker can escalate his privileges by poisoning the Cookie from GUEST to ADMIN to effectively become Administrator or poisoning to ZSL to become Super Administrator.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter Remote Authentication Removal
Electrolink FM/DAB/TV Transmitter suffers from an unauthenticated parameter manipulation that allows an attacker to set the credentials to blank giving her access to the admin panel. It is also vulnerable to account takeover and arbitrary password change.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter (Login Cookie) Authentication Bypass
Electrolink FM/DAB/TV Transmitter suffers from an authentication bypass vulnerability affecting the Login Cookie. An attacker can set an arbitrary value except NO to the Login Cookie and have full system access.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter (controlloLogin.js) Credential Disclosure
Electrolink FM/DAB/TV Transmitter suffers from a disclosure of clear-text credentials in controlloLogin.js that can allow security bypass and system access.
- Link
—
” “Mon, 02 Oct 2023
Electrolink FM/DAB/TV Transmitter (login.htm/mail.htm) Credential Disclosure
The Electrolink FM/DAB/TV Transmitter suffers from a disclosure of clear-text credentials in login.htm and mail.htm that can allow security bypass and system access.
- Link
—
” “Mon, 02 Oct 2023
Juniper SRX Firewall / EX Switch Remote Code Execution
This Metasploit module exploits a PHP environment variable manipulation vulnerability affecting Juniper SRX firewalls and EX switches. The affected Juniper devices running FreeBSD and every FreeBSD process can access their stdin by opening /dev/fd/0. The exploit also makes use of two useful PHP features. The first being auto_prepend_file which causes the provided file to be added using the require function. The second PHP function is allow_url_include which allows the use of URL-aware fopen wrappers. By enabling allow_url_include, the exploit can use any protocol wrapper with auto_prepend_file. The module then uses data:// to provide a file inline which includes the base64 encoded PHP payload. By default this exploit returns a session confined to a FreeBSD jail with limited functionality. There is a datastore option JAIL_BREAK, that when set to true, will steal the necessary tokens from a user authenticated to the J-Web application, in order to overwrite the root password hash. If there is no user authenticated to the J-Web application this method will not work. The module then authenticates with the new root password over SSH and then rewrites the original root password hash to /etc/master.passwd.
- Link
—
” “Fri, 29 Sep 2023
JetBrains TeamCity Unauthenticated Remote Code Execution
This Metasploit module exploits an authentication bypass vulnerability to achieve unauthenticated remote code execution against a vulnerable JetBrains TeamCity server. All versions of TeamCity prior to version 2023.05.4 are vulnerable to this issue. The vulnerability was originally discovered by SonarSource.
- Link
—
” “Fri, 29 Sep 2023
Microsoft Windows Kernel Refcount Overflow / Use-After-Free
The Microsoft Windows kernel does not reset security cache during self-healing, leading to refcount overflow and use-after-free conditions.
- Link
—

” “Wed, 27 Sep 2023
Microsoft Error Reporting Local Privilege Elevation
This Metasploit module takes advantage of a bug in the way Windows error reporting opens the report parser. If you open a report, Windows uses a relative path to locate the rendering program. By creating a specific alternate directory structure, we can coerce Windows into opening an arbitrary executable as SYSTEM. If the current user is a local admin, the system will attempt impersonation and the exploit will fail.
- Link
—
” “Mon, 25 Sep 2023
RoyalTSX 6.0.1 RTSZ File Handling Heap Memory Corruption
RoyalTSX version 6.0.1 suffers from an RTSZ file handling heap memory corruption vulnerability. The application receives SIGABRT after the RAPortCheck.createNWConnection() function is handling the SecureGatewayHost object in the RoyalTSXNativeUI. When the hostname has an array of around 1600 bytes and the Test Connection is clicked the application crashes instantly.
- Link
—
” “Mon, 25 Sep 2023
OPNsense 23.1.11_1 / 23.7.3 / 23.7.4 Cross Site Scripting / Privilege Escalation
OPNsense versions 23.1.11_1, 23.7.3, and 23.7.4 suffer from cross site scripting vulnerabilities that can allow for privilege escalation.
- Link
—
” “Mon, 25 Sep 2023
LogoBee CMS 0.2 Cross Site Scripting
LogoBee CMS version 0.2 suffers from a cross site scripting vulnerability.
- Link
—
” “Mon, 25 Sep 2023
Lamano LMS 0.1 Insecure Settings
Lamano LMS version 0.1 suffers from an ignored default credential vulnerability.
- Link
—
” “Fri, 22 Sep 2023
Elasticsearch 8.5.3 Stack Overflow
Elasticsearch version 8.5.3 stack overflow proof of concept exploit.
- Link
—
” “Fri, 22 Sep 2023
Taskhub 2.8.8 Cross Site Scripting
Taskhub version 2.8.8 suffers from a cross site scripting vulnerability.
- Link
—
” “Thu, 21 Sep 2023
TOTOLINK Wireless Routers Remote Command Execution
Multiple TOTOLINK network products contain a command injection vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary commands through the command parameter. After exploitation, an attacker will have full access with the same user privileges under which the webserver is running - which is typically root.
- Link
—
”

0-Day

“Wed, 04 Oct 2023
ZDI-23-1526: (0Day) MuseScore CAP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Wed, 04 Oct 2023
ZDI-23-1525: (0Day) D-Link DIR-X3260 SetSysEmailSettings SMTPServerAddress Command

Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1524: (0Day) D-Link DIR-X3260 SetSysEmailSettings AccountPassword Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1523: (0Day) D-Link DIR-X3260 SetSysEmailSettings AccountName Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1522: (0Day) D-Link DIR-X3260 SetSysEmailSettings EmailTo Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1521: (0Day) D-Link DIR-X3260 SetTriggerPPPoEValidate Password Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1520: (0Day) D-Link DIR-X3260 SetSysEmailSettings EmailFrom Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1519: (0Day) D-Link DIR-X3260 SetTriggerPPPoEValidate Username Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1518: (0Day) D-Link DIR-X3260 prog.cgi Incorrect Implementation of Authentication Algorithm Authentication Bypass Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1517: (0Day) D-Link DIR-X3260 Prog.cgi Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1516: (0Day) D-Link DIR-X3260 Prog.cgi Heap-based Buffer Overflow Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1515: (0Day) D-Link DAP-2622 DDP Set IPv4 Address Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1514: (0Day) D-Link DAP-2622 Telnet CLI Command Injection Remote Code Execution Vulnerability
- Link

—

” “Wed, 04 Oct 2023
ZDI-23-1513: (0Day) D-Link Multiple Routers cli Command Injection Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1512: (0Day) D-Link D-View coreservice_action_script Exposed Dangerous Function Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1511: (0Day) D-Link D-View shutdown_coreserver Missing Authentication Denial-of-Service Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1510: (0Day) D-Link D-View addDv7Probe XML External Entity Processing Information Disclosure Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1509: (0Day) D-Link D-View InstallApplication Use of Hard-coded Credentials Authentication Bypass Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1508: (0Day) D-Link D-View showUsers Improper Authorization Privilege Escalation Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1507: (0Day) D-Link DAP-1325 SetSetupWizardStatus Enabled Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1506: (0Day) D-Link DAP-1325 SetAPLanSettings IPAddr Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1505: (0Day) D-Link DAP-1325 SetAPLanSettings Gateway Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1504: (0Day) D-Link DAP-1325 SetAPLanSettings DeviceName Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1503: (0Day) D-Link DAP-1325 get_value_of_key Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1502: (0Day) D-Link DAP-1325 get_value_from_app Stack-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Wed, 04 Oct 2023

ZDI-23-1501: (0Day) D-Link DAP-1325 HNAP SetWLanRadioSettings Channel Command Injection Remote Code Execution Vulnerability

- Link

—
” “Wed, 04 Oct 2023
ZDI-23-1500: Cacti graph_view SQL Injection Authentication Bypass Vulnerability
- Link
—
” “Wed, 04 Oct 2023
ZDI-23-1499: Cacti link Local File Inclusion Remote Code Execution Vulnerability
- Link
—
” “Wed, 04 Oct 2023
ZDI-23-1498: Ansys SpaceClaim X_B File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
” “Wed, 04 Oct 2023
ZDI-23-1497: Apple iTunes Incorrect Permission Assignment Privilege Escalation Vulnerability
- Link
—
” “Wed, 04 Oct 2023
ZDI-23-1496: A10 Thunder ADC FileMgmtExport Directory Traversal Arbitrary File Read and Deletion Vulnerability
- Link
—
” “Wed, 04 Oct 2023
ZDI-23-1495: A10 Thunder ADC ShowTechDownloadView Directory Traversal Information Disclosure Vulnerability
- Link
—
”

Die Hacks der Woche

mit Martin Haunschmid

Good Guy Debugmodus deanonymisiert einen Ransomware-Programmierer | Die webp-Lücke

Zum Youtube Video

Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2023-10-03	Metro Transit	[USA]	Link
2023-10-02	Estes Express Lines	[USA]	Link
2023-10-02	Hochschule de Karlsruhe	[DEU]	Link
2023-10-02	Provincia di Cosenza	[ITA]	Link
2023-10-02	Degenia	[DEU]	Link
2023-10-01	Lyca Mobile UK	[GBR]	Link

Ransomware-Erpressungen: (Okt)

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