Cross-Origin Information Disclosure via Unauthenticated REST API (/api/4) due to Permissive CORS in Glances

High **nicolargo** published **GHSA-gfc2-9qmw-w7vh** 2 days ago

Package

glances

Affected versions

<= 4.5.2

Patched versions

> 4.5.2

Description

Summary

The Glances web server exposes a REST API (`/api/4/*`) that is accessible without authentication and allows cross-origin requests from any origin due to a permissive CORS policy (`Access-Control-Allow-Origin: *`).

This allows a malicious website to read sensitive system information from a running Glances instance in the victim's browser, leading to cross-origin data exfiltration.

While a previous advisory exists for XML-RPC CORS issues, this report demonstrates that the REST API (`/api/4/*`) is also affected and exposes significantly more sensitive data.

Details

When Glances is started in web mode (e.g., `glances -w -B 0.0.0.0`), it exposes a REST API endpoint at:
http://:61208/api/4/all
The server responds with:
Access-Control-Allow-Origin: *

This allows any origin to perform cross-origin requests and read responses.

The `/api/4/all` endpoint returns extensive system information, including:

- Process list (`processlist`)
- System details (hostname, OS, CPU info)
- Memory and disk usage
- Network interfaces and IP address
- Running services and metrics
  Because no authentication is required by default, this data is accessible to any web page.

PoC

1. Start Glances:
   glances -w -B 0.0.0.0

2. Create a malicious HTML file:

```
<!DOCTYPE html>
<html>
<body>
<script>
fetch("http://<victim-ip>:61208/api/4/all")
  .then(r => r.json())
  .then(data => {
    console.log("DATA:", data);
  });
</script>
</body>
</html>
```

2. Open the file in a browser while Glances is running.
3. Observe that the browser successfully retrieves sensitive system information from the API.
   This works cross-origin (e.g., from file:// or attacker-controlled domains).

Impact

A remote attacker can host a malicious website that, when visited by a victim running Glances, can:

- Read sensitive system information
- Enumerate running processes
- Identify network configuration and IP addresses
- Fingerprint the host system

This requires no authentication and no user interaction beyond visiting a web page.
This represents a cross-origin information disclosure vulnerability and can aid further attacks such as reconnaissance or targeted exploitation.

Severity

High

CVE ID

CVE-2026-34839

Weaknesses

▶ CWE-200

Credits

 **Venukamatchi** Reporter