Arbitrary internal service access via /v1/sys/proxy when Cloudflare Tunnel is enabled on ZimaOS

Critical **atopos31** published **GHSA-vqqj-f979-8c8m** 2 weeks ago

Package

https://github.com/IceWhaleTech/ZimaOS/ (ZimaOS)

Affected versions	Patched versions
<=1.5.0	1.5.3

Description

Summary

A proxy endpoint (/v1/sys/proxy) exposed by ZimaOS's web interface can be abused (via an externally reachable domain using a Cloudflare Tunnel) to make requests to internal localhost services. This results in unauthenticated access to internal-only endpoints and sensitive local services when the product is reachable from the Internet through a Cloudflare Tunnel.

Impact

- An unauthenticated remote attacker can use the exposed proxy endpoint to issue requests to internal services bound to localhost or internal-only IPs on the device.
- This can expose sensitive internal endpoints (e.g., user management endpoints, service banners, device configs) that are intended to be accessible only from the local network.
- Potential impacts include: information disclosure (sensitive config, tokens), unauthorized access to admin APIs, and remote discovery of internal services.

POC

Arbitrary internal service access via /v1/sys/proxy when Cloudflare Tunnel is enabled on ZimaOS

Exploit

Exploit.py

Severity

Critical 9.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE ID

CVE-2026-28798

Weaknesses

▶ CWE-918

Credits

DrDark1999 Reporter