Advisory

Issue Date 21 November 2024

TLP: CLEAR

Information in this report has been given a Traffic Light Protocol (TLP) of CLEAR

CLEAR **Public** - May be distributed freely, without restriction.

Severe Vulnerability Found in PAN-OS Management Interface: CVE-2024-0012

Introduction

A critical authentication bypass vulnerability, CVE-2024-0012, affects the management web interface of Palo Alto Networks devices running PAN-OS. It allows unauthenticated attackers administrator-level access, enabling actions like configuration tampering and exploiting other vulnerabilities. The flaw primarily affects systems with management interfaces exposed to external networks.

Detail

CVE-2024-0012 has a CVSSv4 score of 9.3 for internet-exposed interfaces. Exploitation grants attackers administrative privileges, potentially enabling further exploitation through authenticated vulnerabilities, including CVE-2024-9474, which facilitates privilege escalation.

Limited exploitation of CVE-2024-0012 has been observed, with attackers targeting management web interfaces exposed to internet traffic. Palo Alto Networks' Unit 42 has detailed Indicators of Compromise (IoCs) and exploitation patterns, underlining the urgent need for mitigation.

Recommendations

- **Verify affected devices,** see PAN-SA-2024-0015 advisory.
- **Adopt workaround and mitigations** that include securing the management interface by limiting access to trusted internal systems
- **Block attacks using Threat IDs 95746, 95747, 95752, 95753, 95759, and 95763,** if subscribed to Threat Prevention.
- **Monitor IoCs**: Use the Unit 42 vulnerability threat brief to detect potential exploitation attempts.

For further details, please refer to the Palo Alto's Security Advisory and Best Practice Deployment Guidelines

If you have any concerns, or have been affected by a cyber-related issue, report it to the CSC by submitting a Cyber Concerns Online Reporting Form at https://csc.gov.im

TLP: CLEAR