



143

**VULNERABILITIES
FOR THE MONTH**

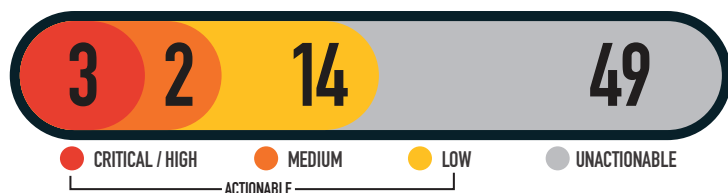
64

**RESEARCHERS
SINCE LAUNCH**

68

**ACTIONABLE REPORTS
PROCESSED**

SEVERITY FOR THE MONTH



100%

MITIGATIONS FOR THE MONTH

- **12 Successful Mitigations**
(Including Top 5 Organization Data)
- **0 Unsuccessful Attempts**

KNOWLEDGE BYTE

DIB-VDP received notification of an asset vulnerable to CVE-2024-3400, a command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software. Specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the appliance. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. The most common resolution for this issue has been implemented in the hotfix releases of PAN-OS versions 10.2.9-h1, 11.0.4-h1, and 11.1.2-h3, as well as in all subsequent PAN-OS versions. More information is available at:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-3400>
<https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/>
<https://vulcan.io/blog/fixing-cve-2024-3400/>

RESEARCHER OF THE MONTH

🔍 New Discovery! 🔍 [@drabdalrhamn9](#) has found a critical opening within a JSON Web Token. This vulnerability (CVSS 9.8) allows unauthenticated attackers to gain Admin entry via Token manipulation. Ensure your systems are secure! #CyberSecurity #InfoSec #OracleWebLogic

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH

