Network Security Package for ioPAC 6500 Series (65M) Firewall Modules Release Notes

Version: v19.0.15	Build: 26112417
Release Date: Nov 28, 2026	

Applicable Products

ioPAC 6500 Series (65M) Firewall Modules

Supported Operating Systems

N/A

New Features

• Added support for IPS pattern v1.213.
• [WordPress WP Statistics Plugin] UserAgentService.php stored XSS vulnerability mitigated. (CVE-2026-48839) (Pattern ID: 1233543)
• [Google Brotli Decoder] Out-of-bounds write vulnerability mitigated. (CVE-2026-111497) (Pattern ID: 1233552)
• [Zoho ManageEngine DataSecurity Plus] Reports SQL injection vulnerability mitigated. (CVE-2026-18912) (Pattern ID: 1233559)
• [Atlassian Multiple Products] Directory traversal vulnerability mitigated. (CVE-2026-21589) (Pattern ID: 1233564)
• [Microsoft Windows] XML XPath translate heap buffer overflow vulnerability mitigated. (CVE-2026-83935) (Pattern ID: 1233565)
• [Oracle Java SE] HotSpot Base64 Decoder heap buffer overflow vulnerability mitigated. (CVE-2026-114938) (Pattern ID: 1233579, 1233580, 1233581)

Enhancements

N/A

Bugs Fixed

N/A

Changes

• The following IPS patterns have been modified or updated to improve system efficiency:
  - [Spotify] SSL access classification signature updated. (Pattern ID: 1063216)

Notes

• The following outdated or deprecated IPS patterns have been removed to improve system efficiency and focus on relevant threats:
  - [NetBSD tnftp] fetch.c fetch_url command execution vulnerability (CVE-2014-8517) (Pattern ID: 1130244)
  - [GitLab Community and Enterprise Edition] Profile Page stored XSS vulnerability (CVE-2024-1451) (Pattern ID: 1232414)
  - [LogMeIn] SSL access classification signature (Pattern ID: 1065942)
  - [WordPress WPvivid Backup] Cross-site scripting vulnerability (CVE-2024-4439) (Pattern ID: 1232401)
  - [F5 BIG-IP Next Central Manager] API injection vulnerability (CVE-2024-21793, CVE-2024-26026) (Pattern ID: 1232406, 1232407)
  - [WordPress WPvivid Backup Plugin] PHAR insecure deserialization vulnerability (CVE-2024-3054) (Pattern ID: 1232395)
  - [Varnish Cache] HTTP/2 flow control denial-of-service vulnerability (CVE-2024-30156) (Pattern ID: 1232398)

- [Torrentpier] Search Query insecure deserialization vulnerability (CVE-2024-1651) (Pattern ID: 1232399)