

SMX-PSA-2026-001

Draft example: libpng vulnerability in QNX 6.5-based products

This worked example uses CVE-2026-25646 and the Servomex products identified for the mock. Exact product releases, part numbers, exposure and download routes require Engineering and PSIRT approval.

Advisory	Version	Lifecycle	Severity	Published	Last updated
SMX-PSA-2026-001	2.1-draft	Closed	High	Draft - not published	1 September 2026

Customer action

Download and install the approved product software version listed below.

Assessment, remediation status and customer action are deliberately separate. For example: Known affected; Fix available; Download and install this version.

Product applicability and remediation

Product or product range	Platform / component	Affected versions	Assessment / remediation	Customer action
2500F Model: 2500F Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.
Laser 3 Plus Model: Laser 3 Plus Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.

Product or product range	Platform / component	Affected versions	Assessment / remediation	Customer action
Multi TX Model: Multi TX Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.
4100 Model: 4100 Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.
4200 Model: 4200 Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.
Multi Gas 4900 Model: Multi Gas 4900 Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.
DF150E Model: DF150E Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.
DF300E Model: DF300E Part numbers: confirm with Servomex	QNX 6.5 variants - exact scope to be confirmed libpng within the software image	Releases containing an affected libpng version - exact range to be confirmed	Known affected Fix available Fixed/recommended release: insert before publication	Download and install this version.

Vulnerability details

CVE	CVE-2026-25646
CWE	CWE-125: Out-of-bounds Read
CNA CVSS	7.0 High - CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H
Known exploitation	No known exploitation - confirm before publication
Attack requirements	The product must call the affected API while processing attacker-controlled PNG palette data; validate the available product input path.
Remediation status	Fix available - product software update incorporating the applicable fix

Summary

libpng versions before 1.6.55 contain an out-of-bounds read in `png_set_quantize()`. This demonstration assumes the affected library is present in the listed QNX 6.5 product software images. Servomex must confirm product-level reachability, credible impact and exact affected releases before publication.

Temporary mitigation

1. Do not transfer or process PNG files from untrusted sources.
2. Restrict product access and file-transfer mechanisms to authorised users and systems.
3. Contact Servomex Support if you cannot determine whether your installed release is affected.

Revision history

Version	Date	Change
2.1-draft	1 September 2026	Aligned the example with CVE-2026-25646 and separated product assessment, remediation status and customer action.
2.0-draft	1 September 2026	Introduced the libpng/QNX 6.5 portfolio example.
1.1	1 September 2026	Initial format demonstration.

Contact: Potential vulnerabilities should be reported to psirt@servomex.com under the Servomex Vulnerability Disclosure Policy. The published web page, not a downloaded PDF, should remain the authoritative current advisory.