GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

2 September 2026

Advisory 235: Pyramid Solutions NetStaX EtherNet/IP Stack Silent Buffer Overflow Vulnerability (CVE-2026-78012).

Release Date: 1st September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate industrial automation or control-system equipment built using Pyramid Solutions' NetStaX EtherNet/IP Stack or EtherNet/IP Adapter DLL Kit (EIPA) — for example, utility, port, manufacturing, or other operational-technology environments running EtherNet/IP-connected adapters, scanners, or controllers. This alert is intended to be understood by technical users and systems/OT administrators.

What is it?

CVE-2026-78012 (CVSS 3.1 base score 9.8, Critical, CWE-121: Stack-based Buffer Overflow) affects the NetStaX EtherNet/IP Stack (also distributed as the EtherNet/IP Adapter DLL Kit, EIPA) developed by Pyramid Solutions, which is embedded by device manufacturers into industrial adapters, scanners, and control systems that speak the EtherNet/IP industrial protocol. A large Class 3 explicit-message request can silently exceed the application-side receive buffer without generating any error or warning back to the sender, resulting in memory corruption, a device crash, or a potential remote attack vector. No privileges or user interaction are required to exploit it.

CVE-2026-78012 was disclosed on 1 September 2026, with Pyramid Solutions publishing a fixed release (NetStaX v5.6.1) on 18 August 2026 ahead of public disclosure. Because NetStaX/EIPA is a development kit embedded into other vendors' end products rather than a standalone application, the

practical exposure for any organization depends on which of its industrial devices were built on an affected version of the stack.

What are the systems affected?

The following version(s) are affected:

- Devices and applications built on Pyramid Solutions NetStaX EtherNet/IP Stack / EtherNet/IP Adapter DLL Kit (EIPA) prior to v5.6.1 – (Affected)

Pyramid Solutions NetStaX v5.6.1 and later – (Not affected, patched)

CERTVU verify Pyramid Solutions' own security bulletin, published directly on its website, is the authoritative source for this vulnerability and was independently fetched and confirmed; however, because NetStaX/EIPA is licensed to device manufacturers and embedded into their own products, the fixed stack version alone does not tell an organization which of its specific devices are affected.

What does this mean?

Typical attack flow:

1. **Reach an affected EtherNet/IP device**
    - An attacker identifies a device built on an affected version of the NetStaX/EIPA stack that is reachable over the network, such as an industrial adapter, scanner, or controller connected to an operational-technology network.
2. **Send an oversized Class 3 explicit-message request**
    - The attacker sends a large Class 3 explicit-message request that exceeds the application-side receive buffer; because the network layer does not validate available buffer space, the device generates no error and instead silently suffers memory corruption, potentially crashing or becoming a foothold for further attack, with no authentication or user interaction required.

Attack vectors:

- Network access to any device built on an affected NetStaX/EIPA version — no authentication, prior access, or user interaction is required.
- Particular risk on flat operational-technology networks where EtherNet/IP devices are reachable from IT networks or the internet, rather than isolated on a segmented OT network.

Successful exploitation may allow attackers to:

- Cause memory corruption or a crash on the affected industrial device, silently and without any error indication to the attacker's own tooling being blocked.
- Potentially achieve a remote attack vector against the device beyond a simple denial of service, with downstream risk to the physical process or operational function that device supports.

Mitigation process

CERTVU recommends the following:

1. Identify affected devices

- Because NetStaX/EIPA is embedded by other manufacturers into their own products, contact the vendor of each EtherNet/IP-connected device in your environment to confirm whether it is built on an affected stack version and whether a firmware or software update incorporating NetStaX v5.6.1 or later is available.

2. Apply vendor firmware updates without delay
3. Restrict network exposure of EtherNet/IP devices pending patching
4. Audit the operational-technology estate
5. Conduct a compromise assessment

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://pyramidsolutions.com/netstax-v-5-6-1-protecting-against-silent-buffer-overflow-in-ethernet-ip-stack-explicit-messages/
2. https://www.cve.org/CVERecord?id=CVE-2026-78012