Vulnerability Incident Response Advisory

To: Ross Technical Support, Product Teams, Sales Managers and Cloud Services

Re: CVE-2026-111497 HIGH SEVERITY Node.js Brotli Decoder RCE

Date issued: 08:00 ET 10/27/2026.

How to use this Advisory

This is an internal only document that is shared with customer-facing staff to help them respond to customer questions about the vulnerability it addresses. Please regard it as the single source of truth on this matter and take care to ensure you're using the most recent version of it. It has been written with customers as the intended audience. You may copy/paste into customer communications from the Customer Advisory section onwards.

As a Vulnerability Incident Response Advisory, it means that Ross Video has determined which products are affected based on the current product vulnerability impact assessment, identified mitigation guidance, and documented follow-up actions for the impacted products.

Note: Advisories such as this one are subject to frequent change. Please use the link below to refresh your copy to ensure you have the most recent version of this document.

CVE-2026-111497 - Node.js - Vulnerability_Incident_Response_Advisory.docx

Customer Advisory

CVE-2026-111497 is a high severity vulnerability in the Brotli decoder bundled with Node.js.

The Node.js security release identifies Node.js 22.x, 24.x, and 26.x before the fixed versions as affected. Exposure depends on whether an affected runtime is shipped or used and whether the product processes attacker-controlled Brotli data.

You can find information about this vulnerability on the Node.js and NIST website here:
https://nodejs.org/en/blog/vulnerability/october-2026-security-releases
https://nvd.nist.gov/vuln/detail/cve-2026-111497

Ross Video's Vulnerability Incident Response Team has been investigating the impact of this vulnerability and has created this communication to help you better understand what is affected and how to respond if needed.

The following Ross Video products are potentially impacted based on the presence of the vulnerable component; however, there is currently no evidence of active exploitation affecting these products

Affected Product/s

Product	Affected version / component	Mitigation / Current status	Patch Release Available
Brushback	V3.0 and prior	No Current mitigation	Awaiting release from Electron with Node 22.23.4 / 24.22.1 **Date TBD**
Carbonite HyperMax	V12.10 and prior	Node.js is present but server does not decode client-supplied Brotli payloads	Node.js update planned — **Date TBD**
XPression.cloud - CPS	CPS 0.4.1, 0.4.2, 0.4.3	Use network/access restrictions.	**Date TBD**
Transitively Affected			
		None	

Sincerely,
Ross Video Vulnerability Incident Response Team, security@rossvideo.com

Our Commitment to Product Security

The number one commitment in our code of ethics is that “We will always act in our customer’s best interests” which is why we take the information security posture of our products and services very seriously at Ross Video.
In practical terms this means that we are constantly monitoring security information channels for alerts about new and serious exploits. When warranted by the criticality and impact to our customers, our Vulnerability Incident Response Team is triggered to analyze whether and how our products are affected, identify mitigation actions, and share this information with our customers.
For further info contact our product security experts at security@rossvideo.com