corero [NETWORK SECURITY]

Corero Network Security

Advisory of Corero Impact from Node.js Chaindrop npm Work

Advisory ID: 08252026-1
Published: 25 Aug 2026
CVEs: n/a

Summary

ChainDrop is a threat campaign, poisoning hundreds of JavaScript packages in the node.js npm registry.

ChainDrop is the umbrella name for an attack using a npm supply chain worms. The attack started through compromised credentials, which then allowed leverage of npm publishing tokens to inject malicious hooks into packages, bump their patch version, and republish.

The exposure was stopped through a combination of revoking tokens, account freezes, removal of poisoned packages, and block listing Command/Control of the worm. This means no new packages could become exposed by this particular worm.

The final impact assessment was 444 packages were poisoned, across more than 1300 unique versions.

Impact Statement

Corero products are not affected by ChainDrop.

Corero audited all products that use node.js once the final impact assessment was available and has confirmed no compromised versions have ever been used.

This audit covered:

SmartWall CMS - version 15.0
SmartWall Service Portal - version 3.2
CORE – including the CORE platform, Traffic Analysis, Zero Trust Admission Control applications

Note that SmartWall Network Threat Defense appliances (hardware and software) and SecureWatch Analytics, do not use node.JS.

Please contact your Corero support representative for more information.