

Tool KEV History

IR Packet

Client Company — inventoried tools with confirmed Known Exploited Vulnerabilities history

Generated: 2026-08-25 14:32 Inventory basis: 34 tools (updated 2026-08-19) KEV feed check: 2026-08-25 (CISA)

Read this correctly: this report is *tool-level history*, not a vulnerability scan. FrameworkMapper knows which products you use, not which versions you run — a product with KEV history may be fully patched in your environment. Use this as a triage ordering ("check these first"), never as a finding of exposure.

Products with confirmed KEV history — check patch status first

PRODUCT	CATEGORY	KEV STATUS	TRIAGE SUGGESTION
PerimeterGate VPN Appliance Vendor: SampleNet	Remote access	KEV history — patch availability unconfirmed	Internet-facing remote access with actively exploited history is the highest-priority initial-access hypothesis. Confirm firmware version and patch level immediately; review VPN authentication logs.
EdgeWall NGFW Vendor: SampleSec	Firewall	KEV history — patches available	Verify firmware is at or above the vendor's fixed release. Export config and egress logs for the response team regardless.

FileMover MFT

Vendor:
SampleSoft

File
transfer

KEV history — patches available

Managed file transfer products are frequent data-theft staging points. Confirm version, then review transfer logs for unusual outbound volume.

Rest of inventory

The remaining 31 inventoried tools have no confirmed KEV association in the current feed. Absence of KEV history is not a clean bill of health — it means CISA has not catalogued active exploitation for those products.

KEV matching is human-confirmed at the product level from the CISA Known Exploited Vulnerabilities catalog. This report refreshes when your tool inventory changes or the KEV review queue confirms a new match affecting your tools.