Lowside Intelligence

Criminals are using a vulnerability in FleetDesk route-planning software to break in

Northfield Freight
21 October 2026

TLP:CLEAR

This is a made-up example. Northfield Freight, FleetDesk, Grey Harbour and every other detail in this report are invented to show the format.

Criminals are using a vulnerability in FleetDesk route-planning software to break in

Northfield Freight runs an affected version and should update today

Executive Summary

What happened. Criminals have found a serious vulnerability in FleetDesk, the route-planning software, and are using it to break in without a password. A free update fixes it.

Why it matters to you. You run an affected version, and your FleetDesk login page can be reached from the internet. Other UK haulage and logistics firms are already being targeted.

What to do. Ask whoever looks after your IT to install the update today.

Key Findings:

- FleetDesk versions 7.0 to 7.4.1 are affected, and version 7.4.2 fixes the vulnerability.
- At least 14 UK transport and logistics firms have been targeted since 20 October.
- We have seen no sign that Northfield Freight has been targeted, and your name and logins have not appeared on the criminal sites we watch.

Relevance to Northfield Freight

Your asset profile lists FleetDesk 7.4, which plans your daily deliveries. If it was locked by ransomware, your drivers would have no routes until it was restored.

FleetDesk also holds customer addresses, delivery schedules and driver details, so a break-in could expose information your customers trust you with. [1]

None of the suppliers in your profile has reported a problem linked to this vulnerability. [2]

Technical Analysis

A specially made request sent to the FleetDesk login page lets an attacker run commands on the computer it sits on. In the cases reported so far, the attacker copies data, then starts ransomware, usually within three days. [1][2]

Timeline

- 19 October 2026: FleetDesk confirms the vulnerability. [1]
- 20 October 2026: FleetDesk releases the update, and the first attacks on UK firms are reported. [1][2]
- 21 October 2026: Grey Harbour names two UK logistics firms on its leak site. [4]

Vulnerabilities and Exploits

The vulnerability is recorded as CVE-0000-00001 and FleetDesk rates it 9.8 out of 10. Criminals are sharing the means to use it, though it has not been published openly. [1][3]

You remain exposed until version 7.4.2 is installed. [1]

Strategic Analysis

Haulage firms can't work for long without route planning, and that puts pressure on them to pay quickly. We expect firms of your size and sector to stay a target this year, so it's worth checking you could keep deliveries moving if FleetDesk went down. [2][4]

Attribution

This looks like Grey Harbour, a ransomware group. Nine of its 22 named victims this year are in transport and logistics. We can't be certain, because other groups may be using the same vulnerability. Your response is the same either way. [2][4]

Recommendations

1. Today: update FleetDesk to version 7.4.2.
2. Today: ask whoever looks after your IT to check FleetDesk for the warning signs in the appendix.
3. This week: change the FleetDesk administrator passwords.
4. This week: restrict who can reach the FleetDesk login page from the internet.
5. If anything looks wrong, tell us straight away and we'll help you work out what to do.

Assessment

What we know

FleetDesk has confirmed the vulnerability and the fix. Two independent sources confirm it is being used in attacks. [1][2]

What we think

1. UK transport and logistics firms are being targeted. (confidence: High) [1][2]
2. Northfield Freight is exposed until the update is installed. (confidence: High) [1]
3. Grey Harbour is behind at least some of this. (confidence: Moderate) [2][4]

What we don't know

- How many firms have actually been broken into, as opposed to targeted.
- Whether data was taken from the two firms named on the leak site.

What would change our view

- You are running a different version from the one in your asset profile.
- A warning sign from the appendix is found on your system.

Evidence Basis

This report rests on 9 claims in 4 reports from 3 independent sources. We rate 3 of the claims as confirmed, 4 as probable and 2 as plausible.

References

#	Source	Date	Title
1	FleetDesk	2026-10-19	Security advisory for FleetDesk 7.x
2	Security researcher	2026-10-20	Exploitation of FleetDesk in UK logistics
3	Criminal forum	2026-10-18	Post offering access to a UK haulage firm
4	Grey Harbour leak site	2026-10-21	Leak site listing of two UK logistics firms

Appendices

Warning signs for whoever looks after your IT. All values below are fictional. Technical files, including detection rules, come with each report.

Type	Value	What it is
IP address	203.0.113.42	Source of the attacks
Domain	fleetdesk-update[.]example	Serves the attacker’s remote access tool
File	fdsvc-helper.exe	The remote access tool