Jeppesen Ransomware Attack Update

OPSGROUP Team
14 November, 2022

On November 3rd a ransomware attack took down the majority of **Jeppesen planning products.**

We heard that:

- **Jetplan.com** was down
- **Milplanner.com** was down
- **Jetplanner** (standalone) was not working
- **Chart viewer** products was not working (eg. Elink portal, and Icharts)
- **FliteDeck Pro** was not working
- **Foreflight** (now a Boeing company) was working but their Notam feed was not.

Find the post on this here.

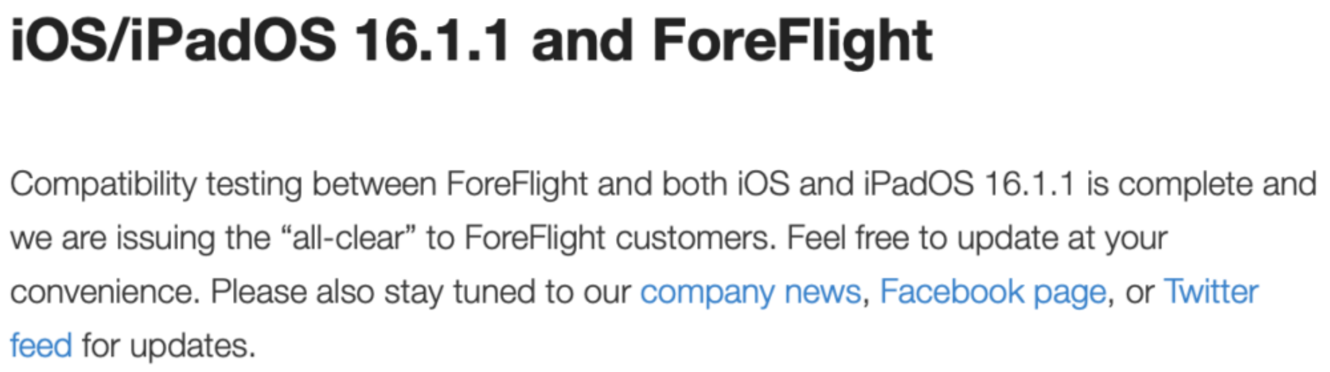
Update: November 16

We asked around and it sounds like it took longer to fix than expected, and some bits still aren't working quite as they were:

- **Foreflight notams** remained down for several days
- **Ice crystal areas** are not showing
- There is an ongoing issue with **expired charts and updates being unavailable**
    - Jeppesen has advised that *"The most recent Jeppesen chart downloads are currently effective and in compliance. Any "expired" messages prior to Dec 1 do not indicate that*

    the charts are expired from a regulatory perspective.”

    - However, they do also have this note up. We suggest checking with them direct if unsure whether to update or not:



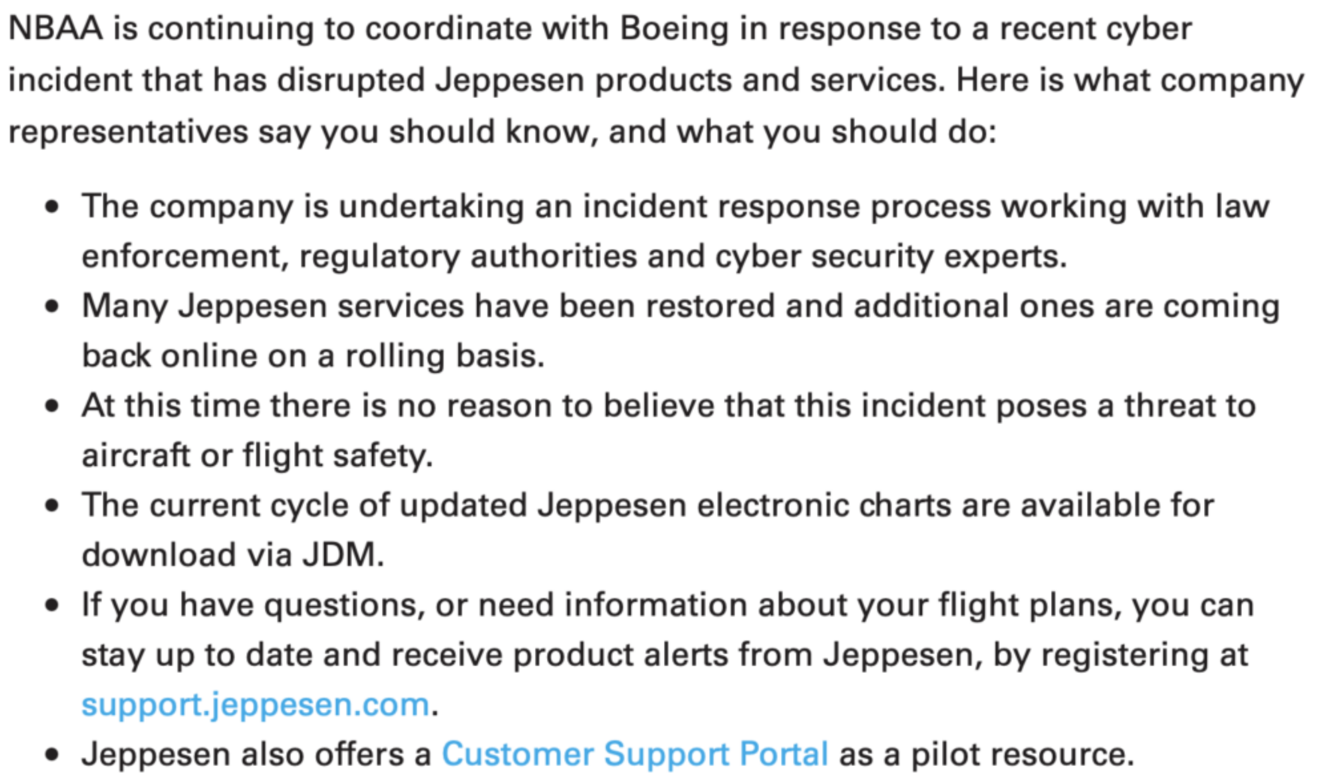
iOS/iPadOS 16.1.1 and ForeFlight

Compatibility testing between ForeFlight and both iOS and iPadOS 16.1.1 is complete and we are issuing the “all-clear” to ForeFlight customers. Feel free to update at your convenience. Please also stay tuned to our company news, Facebook page, or Twitter feed for updates.

Something about updates

You can read their response to the attack here, including an explanation of whether or not you need an update.

The NBAA has also posted this:



NBAA is continuing to coordinate with Boeing in response to a recent cyber incident that has disrupted Jeppesen products and services. Here is what company representatives say you should know, and what you should do:

- The company is undertaking an incident response process working with law enforcement, regulatory authorities and cyber security experts.
- Many Jeppesen services have been restored and additional ones are coming back online on a rolling basis.
- At this time there is no reason to believe that this incident poses a threat to aircraft or flight safety.
- The current cycle of updated Jeppesen electronic charts are available for download via JDM.
- If you have questions, or need information about your flight plans, you can stay up to date and receive product alerts from Jeppesen, by registering at support.jeppesen.com.
- Jeppesen also offers a Customer Support Portal as a pilot resource.

So how big was the impact?

It was pretty big for some. The most disruptive seemingly for those reliant on the planning software.

Let us know if you were impacted (or still are).

What can you do if this happens again?

We aren't sure actually. It raised more questions for us than we have answers for:

- **Can you use old route plans?**
- **Can you use old fuel plans?**
- **Where else can you get weather, Notam and planning info from?**
- **Are there any back-ups for charts?**
- **What else haven't we thought of?**

We've asked the question to members who were impacted by this.

If you were, and have some feedback on what the impact was and what you did about it, then send us the info at team@ops.group We will keep it anonymous, but if you have anything that can help others plan for/mitigate disruption if it occurs again in the future, then we want to hear it.

Has this happened before?

Computer and software glitches have caused numerous issues in the past, but most of these have been **related to passenger booking info.**

A problem with **Aerodata**, which several major US airlines use for weight and balance, caused disruption in 2019.

In 2021, a **cyber attack on a major fuel pipeline** in the USA led to significant disruption at east coast airports due to fuel supply issues.

The cyber security threat.

You’ve probably had to sit through a Cyber Security training thing at your organisation. They are basically common sense: don’t open random links and don’t give out passwords (or information that helps people guess passwords).

Cyber criminal cunningness is increasing though. We wrote about some of it here, and it is worth upping the caution levels and making sure you ain’t a weak link in security.