DC False Alerts: Could TCAS Be Vulnerable to Cyber Attack?

Chris Shieff
10 March, 2025

On March 1, several aircraft reported erroneous TCAS TA and RA alerts while on approach to Runway 19 at **KDCA/Washington.** All aircraft correctly followed avoidance procedures, and **no loss of separation** occurred. Six of the incidents occurred within eleven minutes of each other.

⬆ *shared with permission, courtesy of **VASAviation.***

What has followed is speculation – who, or what, was responsible? It is an answer the FAA is actively seeking.

TCAS interference is rare but can occur. There are several plausible explanations including ground clutter and reflections, software issues and unintentional radio interference.

However, it would be hard to deny that these alerts came at a **sensitive time** both for operations at the airport following the mid-air collision over the Potomac River, and across a broader tapestry of concern for aviation safety across the US NAS given recent events.

Which begs an important question – **can TCAS actually be tampered with?** Is it possible these events were an act of criminal mischief or other mis-intent? While remote, a little-known alert issued just weeks ago by **CISA** (the part of Homeland Security responsible for US cyber and infrastructure security) suggests it is *indeed* possible.

Published on January 21, CISA discussed **two flaws in TCAS design** that leave the system vulnerable to **malicious cyber-attacks** – one of which they deem a high, almost critical vulnerability.

In event that such an attack occurs, criminal interference could generate fake targets on an aircraft's TCAS display and even disable resolution advisories.

The problem is that bulletin is quite technical. So here is a break-down of what it says in plain, simple language.

The Bulletin

There were essentially two risks identified for TCAS II Versions 7.1 or older.

1. Fake Position Signals

It is theoretically possible to broadcast a spoofed aircraft location to another target.

This could be achieved using specialised radio equipment where potential attackers could send fake signals to aircraft, causing the appearance of **non-existent targets** on TCAS displays, along with the associated warnings.

In other words, crews would effectively be chasing shadows.

As TCAS II systems rely on transponders that may not be able to adequately validate the data received, they remain vulnerable to unauthorised signals. The bulletin describes this risk as a reliance on '*untrusted inputs'.*

Read the report and you'll see something called a '**CVSS score.'**

CVSS stands for **Common Vulnerability Scoring System**, and it is basically a danger rating for flaws in computer security. It is a measure of how serious a vulnerability is. Factors include the method of attack, the access required and the potential impact.

It is represented on a scale of 0 (non-existent) to 10 (critical).

The issue of fake position signals has been given a CVSS score of 6.1.

Perhaps more concerning is that the report advises there is no way to actively mitigate this threat with existing TCAS technology. The equipment required is accessible to the public. Therefore this threat is the most likely suspect of any erroneous TCAS interference occurring today.

2. No TCAS RA

This affects some older TCAS II systems using transponders with outdated technical standards.

It is theoretically possible for an attacker to impersonate a ground station and send a special request that lowers a system's sensitivity settings. A TCAS sensitivity level command does exist, envisaged to reduce nuisance alerts at some airports.

This could be used to maliciously adjust sensitivities to the lowest setting and even **disable a resolution advisory** completely.

The threat has a concerning CVSS score of 8.1 – highly vulnerable to exploitation, but would require a high level of expertise and technology to carry out.

Fortunately, in this case there is a way to mitigate the problem – by switching to ACAS X, or upgrading your associated transponder to more recent technical standards.

There is **no indication** that this has vulnerability has ever been exploited.

While unlikely, the CISA bulletin proves that TCAS could be vulnerable to malicious interference.

So, could the aircraft at KDCA have been hacked?

It's unlikely, but CISA's report indicates it's possible. And a new expert analysis of events at KDCA by **Aireon** seems to agree. In their published report they found that *'it is possible the intruder was airborne or related to a ground-based transmitter used for testing or spoofing.'*

Why does this matter?

The industry must remain responsive to security threats that are becoming increasingly sophisticated and designed to exploit vulnerabilities in safety critical systems.

The recent industry-wide interest in GPS interference spanning from the inconvenient, to major degradations including the loss of EGPWS protection, ADS-B tracking and navigational accuracy is a startling testament to this fact. This is all possible because of **existing system design.**

Since the events of September 11, passenger screening and security protocols have undergone a revolution, and it's now much harder for bad actors to carry out conventional attacks. But there are still risks associated with malicious attacks that could potentially be achieved **remotely** – and cyber-interference seems an obvious choice.

Jeppesen Ransomware Attack Update

OPSGROUP Team
10 March, 2025

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:

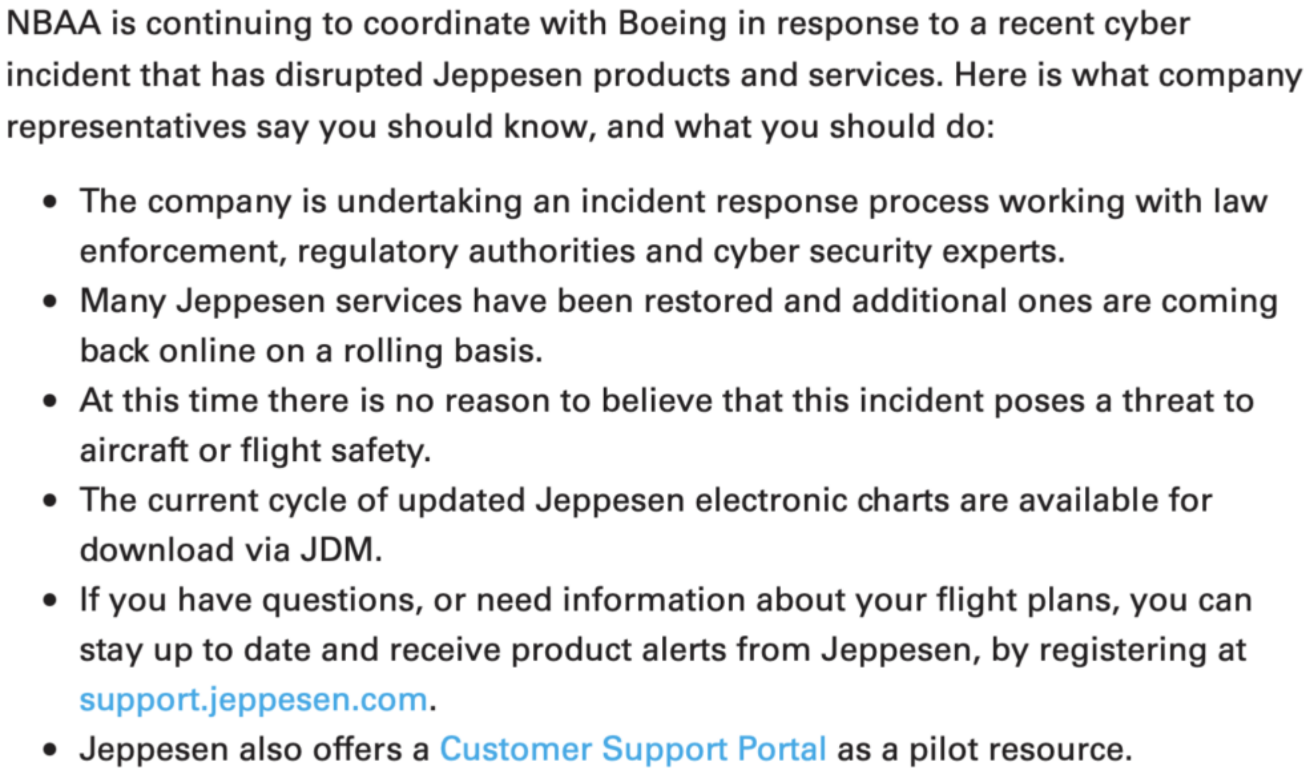
- **Foreflight notams** remained down for several days
- **Ice crystal areas** are not showing
- There is an ongoing issue with **expired charts and updates being unavailable**
    - Jeppesen has advised that *"The most recent Jeppesen chart downloads are currently effective and in compliance. Any "expired"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

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.

Please be Wary of Malicious Phish

OPSGROUP Team
10 March, 2025

There is a new threat to flight ops security, and it might not come from where you think it would.

The Hack Attack

We talked about the threats of airplanes and control towers being hacked before. But now we want to talk about cybersecurity.

Anyone who works for a big company has probably had to do their cybersecurity training at some point. If you haven’t, here is an example. Answers at the bottom of the page.

The trouble is, the scams we have been seeing are getting more and more, well, *smart.*

The Nigerian Prince

The good old Nigerian Prince who wants to give you One Hundred Million Gazillion Dollars scam. **As old as the internet itself.**

How does it work? (And yes, these do still work. Apparently they **rake in over $700,000 a year** from unwitting victims).

In a Kola nutshell, you receive an email from someone overseas (and there are different iterations of this now but it is always along the same lines) – a royal prince is **wanting to give you money,** or a disgustingly rich recluse of a distant uncle has passed away and mentioned you in their will.

Whichever they use, the trick is the same – they supposedly have money for you, and all you need to do is **provide your bank account details** and they will transfer it all over, for a small fee.

Only here is the catch (sorry to break it to you) – There is no Prince, there is no money, and **now they have your bank details** and maybe even a payment you have sent them.

This doesn't affect Flight Ops though?

No, it doesn't. Not really. Unless you count the **Nigerian Astronaut stuck in space** one.

There is also the recent one which the NBAA warned about involving **Imposter CBP Agents** who call private residences and businesses and attempt to gain banking information.

And then there are the **fake websites** offering free tickets or special deals, and steal "passenger" information which they freely provide. [https://deltaairlines-flights.com] is not a legit website. Don't buy tickets from there.

The ones that we want to bring up though are **Phishing scams and Malware emails**.

So, what do you need to be on the look out for, and how do these even **impact Flight Ops and Security?**

Be Wary of Malicious Phish

This is when an email is sent which looks legit. You open it, maybe it tells you there is an iTunes bill you need to pay. You wonder what you bought on iTunes, you can't remember, so **you open the attachment and BAM!**

Malware is sophisticated nowadays. It doesn't always just shut your computer down, or flash up a retro laughing skull icon. It might destroy data, it might steal data. It might install ransomware on your systems.

Hackers recently took hold of an oil pipeline in the USA.

The Colonial Pipeline supplies half of the east coast's fuel supply. Hackers managed to shut it off, probably via an email. The impact was **no fuel supply from Houston to New Jersey** and this affected all the airports along that route. It also led to **increased fuel prices and ongoing impacts** even after the fuel supply was re-established.

Phishing is a similar scam.

An email, or a phone call from **a "trusted source"** appears in your inbox and somehow cons you into into giving login data, passwords, user info. Once access has been "granted" the hacker can do a lot of damage. From **stealing confidential information, to taking control of systems.**

I.T. Operator SITA which serves major Star Alliance airlines such as Lufthansa and Singapore suffered a **data breach in Q1 2021** with hackers gaining access to ticketing and baggage control systems which led to the information of thousands of passengers being stolen.

In 2020, major European regional airline EasyJet admitted an attack may have **compromised data of around 9 million passengers.** Several thousands had their credit and debit card details accessed.

What are we seeing at OPSGROUP?

We are seeing scammers getting more cunning, scams which are more targeted and ones which are **worryingly specific.**

First up, the **Nav Fees scam.** This one has been around for a while – we reported on it here. They send you an email, pretending to be from Eurocontrol or IATA or some government agency, with a new bank account to send your Nav Fees to. Pretty standard stuff. Fortunately, most of these emails are poorly written, and easy enough to identify as bogus – but that’s only if you are on your guard.

Then there’s the **charter quote email scam**. These have believable company names. Some of the names are even “real” people, so the email looks legitimate, and **all it does is ask for a quote.** So you open the email attachment and now they have you.

Thankfully, **OPSGROUP is not in the charter quote business** (and our email system is fairly good at spotting these now), but for some of you reading this, who do see real emails for quotes, this might pose a problem.

The more concerning ones come from very specific, and **very genuine aviation linked companies** such as ‘Airbus’.

These are worrying because they are **so specific, so targeted,** that it is often hard to spot the real from the scam.

Microsoft put a warning out earlier in 2021 saying they are tracking this ‘dynamic’ campaign which is targeting the aerospace and travel sectors with **spear-phishing emails**. When the PDF in the email is opened it delivers RevengeRAT or AsyncRAT to your computer.

RATs it seems are the new worms. A Trojan is installed and user credentials, webcam info, statistics about the system are pilfered and pillaged.

Your OPSGROUP Cybersecurity Assessment

1. If you receive an email from an unknown sender, or for something you haven’t signed up to – should you open the attachment?
   - ○ Yes
   - ○ No
2. You receive an email or a call asking for details that involve passport info, bank details or anything else sensitive – should you share it?
   - ○ Yes
   - ○ No
3. There is a Nigerian Prince/Princess who really wants to marry you and send you several million dollars – should you trust them?

- ○ Yes
- ○ No

If you answered “Yes” to any of these questions, go back to the start of this article and read it again.