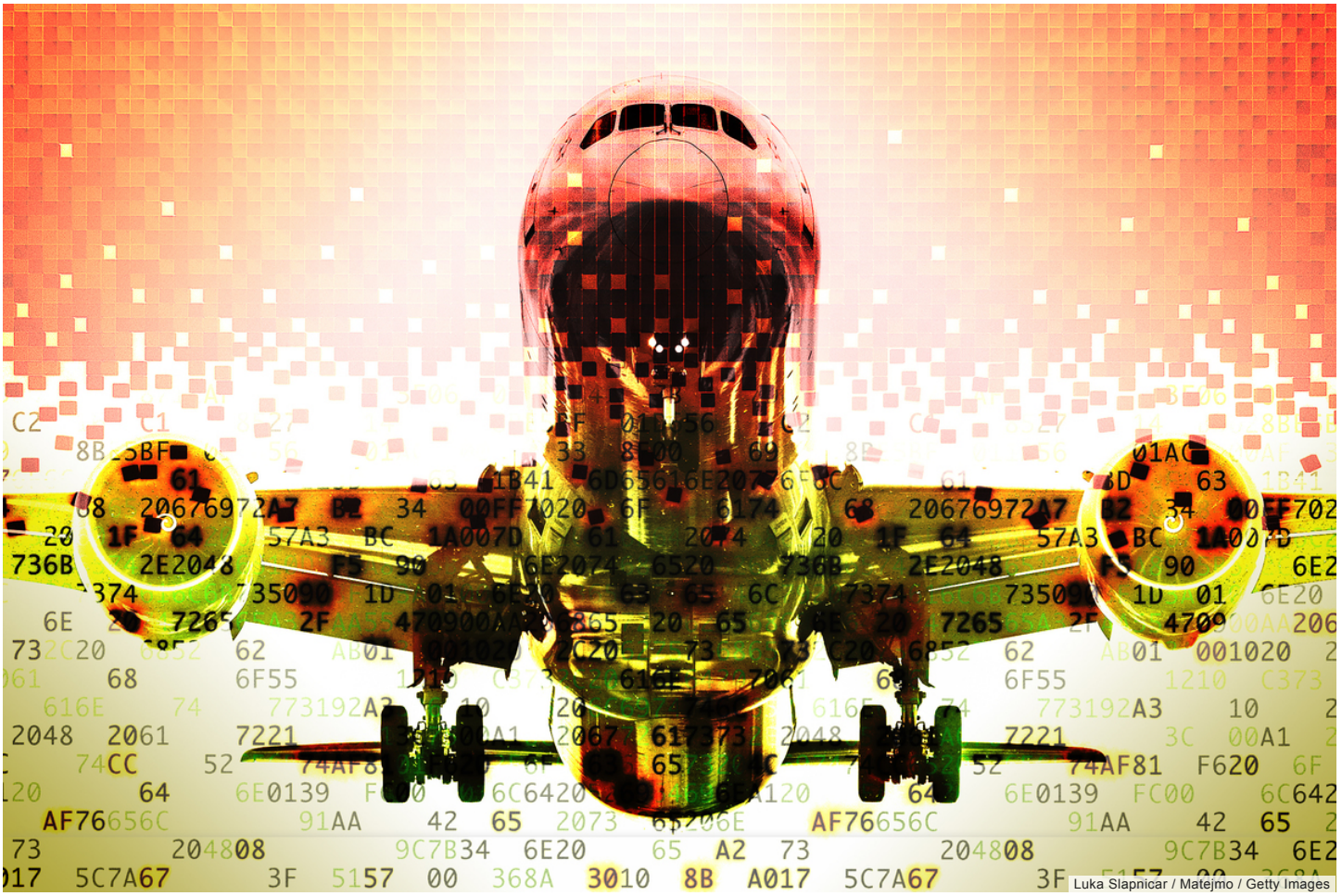
NEWS

Boeing's poor information security posture threatens passenger safety, national security, researcher says

The aircraft maker failed to perform minimum due diligence in securing its networks, then tried to cover it up, security researcher Chris Kubecka tells Aviation Cyber Security conference attendees.

By J.M. Porup
Senior Writer, CSO | NOV 5, 2019 2:00 AM PST


Luka Slapnicar / Matejmo / Getty Images

Boeing's poor information security practices threaten aviation safety and [illegible]s Kubecka told an audience at the Aviation Cyber Security conference in L[illegible]

Boeing test development networks are publicly exposed to the internet, K[illegible] email servers is infected with multiple strains of malware. Kubecka believ[illegible] being used to exfiltrate sensitive intellectual property including code used as aircraft Boeing sells to the US military.

[Editor's note: This article has been updated to add comments from Boeing and the FAA.]


Chris Kubecka

Kubecka, a well-respected security researcher, critical infrastructure expert, and Air Force veteran, tells *CSO* she has struggled to report what she calls blatant, easily fixable security issues for more than six months. She also alleges that Boeing, through back channels at DEF CON, threatened her with legal action and a public relations smear campaign to prevent her from going public. Kubecka declined to identify who made the threats, when and where they were made, or how they might be associated with Boeing.

"If I saw a broken door on an aircraft, I would not get in trouble for reporting to the FAA that the plane flew," Kubecka tells *CSO*. "But as a security researcher, it's legally fraught to report security vulnerabilities."

Kubecka says she discovered these security issues on Boeing's networks in April 2019 but could not find a secure way to contact anyone at Boeing, before tweeting about it in July in frustration. "At the time there was no way to get in touch with anyone who understood what I was talking about in a secure manner," Kubecka tells *CSO*. "I couldn't just send this information in plain text [without using encryption], that would be irresponsible."

In a statement, Boeing told CSO "We sincerely appreciate the time and effort that went into Ms. Kubecka's s research, and we take the concerns she raised seriously, as we continually work to enhance the cybersecurity of our IT systems and products.... As DHS itself has recognized, none of the issues Ms. Kubecka identified are unique to aviation, and we have no indication of a compromise in any aviation system or product that Boeing produces." As this story shows, however, information security vulnerabilities in the aviation industry can threaten aviation security, and evidence from VirusTotal suggests that Boeing systems have been compromised.

Furthermore, Kubecka alleges that the company did not welcome her research and tried to silence her.

Alleged threats and intimidation

Following Kubecka's tweet, the industry threat intelligence information-sharing group, the Aviation Information Sharing and Analysis Center (A-ISAC), whose board members include representative of airlines and aircraft manufacturers, contacted Kubecka. According to emails seen by *CSO*, A-ISAC employee Doug Blough, who also works for Boeing, asked for an in-person meeting with Kubecka in Las Vegas in early August, when the information security conferences DEF CON, Black Hat, and BSides Las Vegas all take place.

Blough came to her Las Vegas hotel room on August 6, 2019 for a scheduled meeting and asked her to sign an NDA, Kubecka says. She refused.

"I tried to stress [to Blough] my motivations were not of a criminal nature but come from a safety angle," Kubecka says. "I was a military aviator [in the US Air Force] and I have some experience with avionics."

A-ISAC CEO Jeff Troy disputes this claim. Troy says that a meeting between Kubecka and Blough occurred in a coffee shop in Las Vegas during Black Hat in August 2019 to discuss the matter but denies that an NDA was requested and any threats were made. "Obviously, we take this allegation [of threats] very seriously," Troy tells *CSO*. "We had conversations, looked over a lot of records and things, and I do not believe this happened." Troy declined to comment on the vulnerabilities disclosed by Kubecka, saying that the A-ISAC does not comment on specific vulnerabilities as a matter of policy, but confirmed that the A-ISAC was aware of the vulnerabilities in question in July of this year.

A Boeing spokesperson confirmed that a company employee, presumably Blough, outlined for Kubecka different "models of responsible disclosure, some that include an NDA between the researcher and the organization, and some that don't," but denied that anyone at the company threatened her.

Boeing's poor information security practices

Kubecka says that after speaking with the A-ISAC representative, Blough, in Las Vegas, later that same day (August 6) she spoke with a representative of DHS and shared her research. Boeing confirmed that DHS subsequently shared Kubecka's research with the company in mid-August, through DHS's vulnerability coordination process.

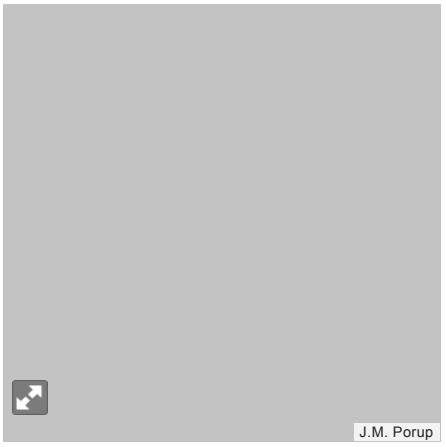
"As part of our typical coordinated disclosure process, the Cybersecurity and Infrastructure Security Agency (CISA) reviewed the report provided by Ms. Chris Kubecka," a CISA official told *CSO* in a statement. "CISA presented the report to Boeing for review and potential remediation.... While we analyze the cybersecurity risks, CISA does not analyze the safety factors potentially created by these vulnerabilities. The sector specific agency is responsible for this analysis."

That would be the Federal Aviation Administration (FAA). An FAA spokesperson told *CSO* that Boeing has a responsibility to secure their networks. "The FAA works with airplane manufacturers to ensure critical airplane systems are protected from Intentional Unauthorized Electronic Interface, which encompasses cybersecurity vulnerabilities. Manufacturers are required to do an environmental scan to assess cyber risks as they apply to their designs and products. Once this assessment is done, the manufacturer presents mitigations to the FAA as part of the certification process for FAA approval. It is incumbent upon the manufacturer to monitor their environment, implement security controls, and ensure that critical systems are protected from malicious activities. Information on manufacturer designs and how they ensure that their critical systems are protected is proprietary."

"Throughout the disclosure, CISA provided a conduit of communication between Boeing and Ms. Kubecka," the CISA official added.

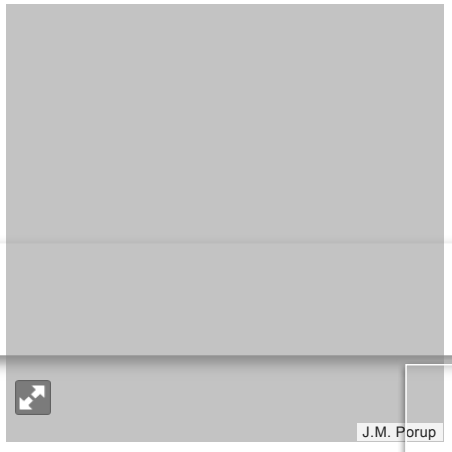
Among a litany of easily remedied security failures, Kubecka reported that Boeing's test development networks were publicly exposed to the internet, potentially enabling a sophisticated adversary to gain access to Boeing software source code and build systems. "Imagine if you are an enemy and you tainted flight control software and suddenly a sensor or detection method didn't work when you go to war with them," Kubecka says. (*CSO* was able to verify that at least one of Boeing's test servers is still online but won't be publishing technical details to avoid helping potential attackers.)

Other basic security precautions that constitute rudimentary due diligence also appear not being followed, including a lack of a TLS certificate (to enable encrypted web traffic via HTTPS) on the Boeing.com website home page, which means a malicious adversary could inject malware into web traffic and infect unsuspecting users. As of last week, more than 90% of web traffic is now encrypted, according to netmarketshare.com, making Boeing an outlier in a sector with known nation-state adversaries. If a company of Boeing's size can't even properly deploy a TLS cert on their website, what other information security lapses might they have committed?



Boeing.com does not deploy HTTPS on their website home page.

Lots, as it turns out. Boeing's email domain also lacks DMARC (Domain-based Message Authentication, Reporting and Conformance). DMARC ensures that only email from legitimate sources reach recipients' inboxes. As a result, it would be easy to spoof email coming from boeing.com, and thus easy to deploy phishing campaigns targeted at Boeing employees, third-party suppliers, or even government customers who interact with Boeing via email. The use of DMARC is now mandatory for all federal government agencies, who are notoriously late adopters of security measures, after DHS ordered all federal agencies to adopt the security practice starting in January, 2018.

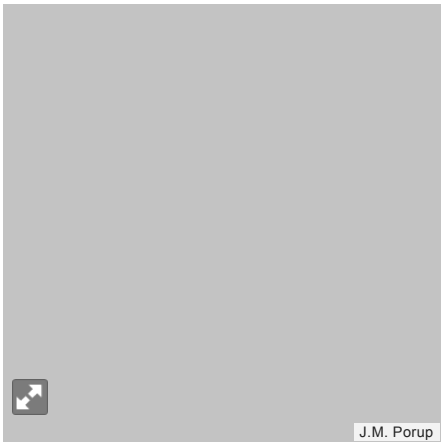


Boeing.com does not use DMARC to prevent email spoofing and phishing attacks.

For example, an attacker could forge a legitimate-looking email from Dennis A. Muilenburg (the CEO of Boeing) that would use the boeing.com domain and ask targeted users to open an attachment containing malware that

would subsequently infect their workstations. DMARC would prevent such an attack, and configuring DMARC is a relatively small undertaking by a competent security professional.

The most damning revelation Kubecka uncovered, however, is that at least one of Boeing's email servers is infected with multiple strains of malware. According to the Virus Total malware database, which is owned and managed by Google, multiple varieties of malware on one of Boeing's email servers are phoning home. Clicking through on the malware hashes listed reveals a wide variety of malware communicating with Boeing's email server when opened or executed.



The red numbers indicate the numbers of antivirus engines that believe the executable in question is malware.

Because of the apparently compromised email servers and lack of DMARC, Kubecka suspects that the infected email servers are being used to exfiltrate sensitive intellectual property, including code used in both civilian passenger aircraft as well as aircraft Boeing sells to the US military.

One of many instances of malware communicating with a Boeing email server.

"Boeing appears to have an issue with email malware security and not blocking outgoing malicious files adequately," Kubecka writes. "There is a high probability that data exfiltration is occurring through the Boeing email servers."

Boeing says they have been working to fix the issues Kubecka uncovered, telling CSO in a statement, "[the company's] information security team has worked diligently to review and resolve each of the reported findings."

However, *CSO* was able to verify that numerous security issues Kubecka reported are still present in Boeing's public facing networks, including a lack of DMARC for their email, and malware communicating with an infected Boeing email server just a few weeks ago.

Boeing's supplier web portal, Aviation ID, also appears rife with security issues, including cross-site scripting (XSS) vulnerabilities, and poor credential and authentication standards, Kubecka said. The portal login code in question is provided by outsourcer Exostar, whose software is widely used in the aviation, space, and defense sectors. Exostar's website boasts the Department of Defense, Ministry of Defense in the UK, Boeing, Embraer, Lockheed Martin, Northrup Grumman, Raytheon, and many other players as clients.

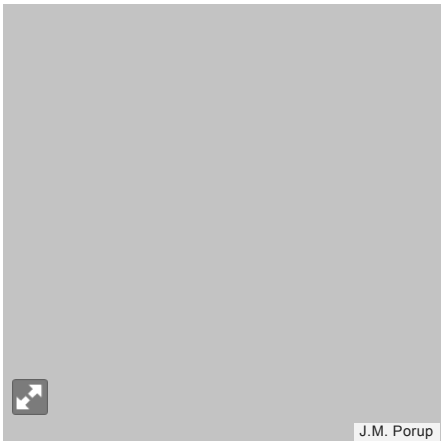
Exostar did not respond to our request for comment. We will update our story if they do.

Boeing botches vulnerability disclosure program

In the last several weeks, Boeing launched a vulnerability disclosure program (VDP) to make it easier for good-faith security researchers to share their findings. "Consistent with industry direction and our broader efforts to engage the security research community," the company said in a statement, "Boeing recently published a vulnerability disclosure policy to enable third parties to securely and responsibly report security vulnerabilities to the company."

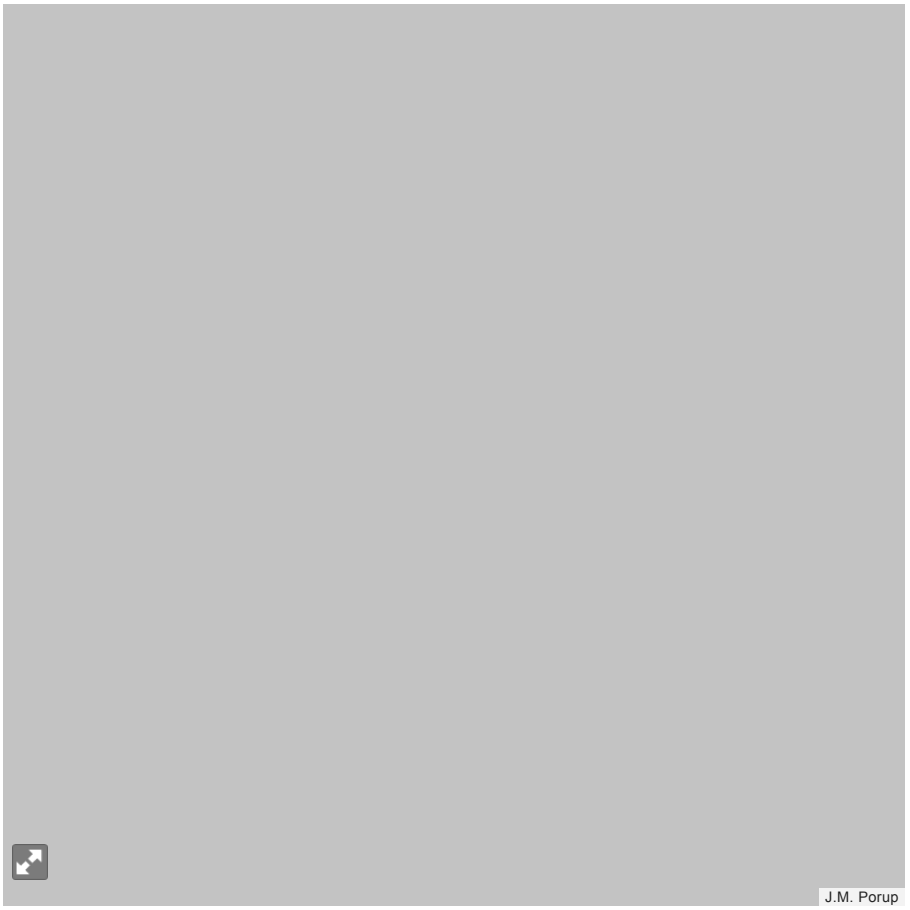
A Boeing spokesperson confirmed that signing "an NDA is not required for researchers to participate in Boeing's vulnerability disclosure policy[sic]." This is a positive step forward. However, other aspects of the new VDP show cause for concern.

Ironically, the VDP web page is not encrypted with a TLS certificate (to enable HTTPS), which means an attacker could identify who is viewing the page, modify the web page to change the reporting email address (VulnerabilityDisclosure@boeing.com) or the PGP key provided. Furthermore, the PGP key posted on their website is an invalid public key. *CSO* tried to use the key to send Boeing a test message but their public key is incorrectly formatted and not recognized as a valid PGP public key.



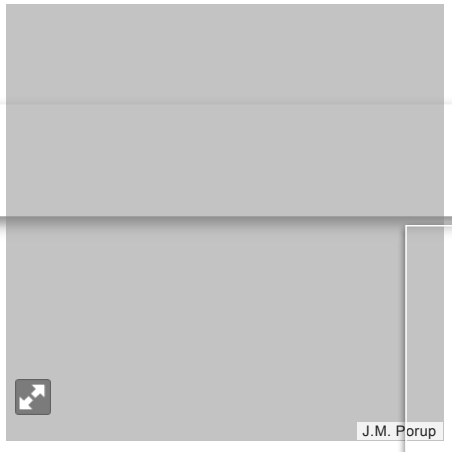
J.M. Porup

Boeing's new VDP is served on an unencrypted web page.



J.M. Porup

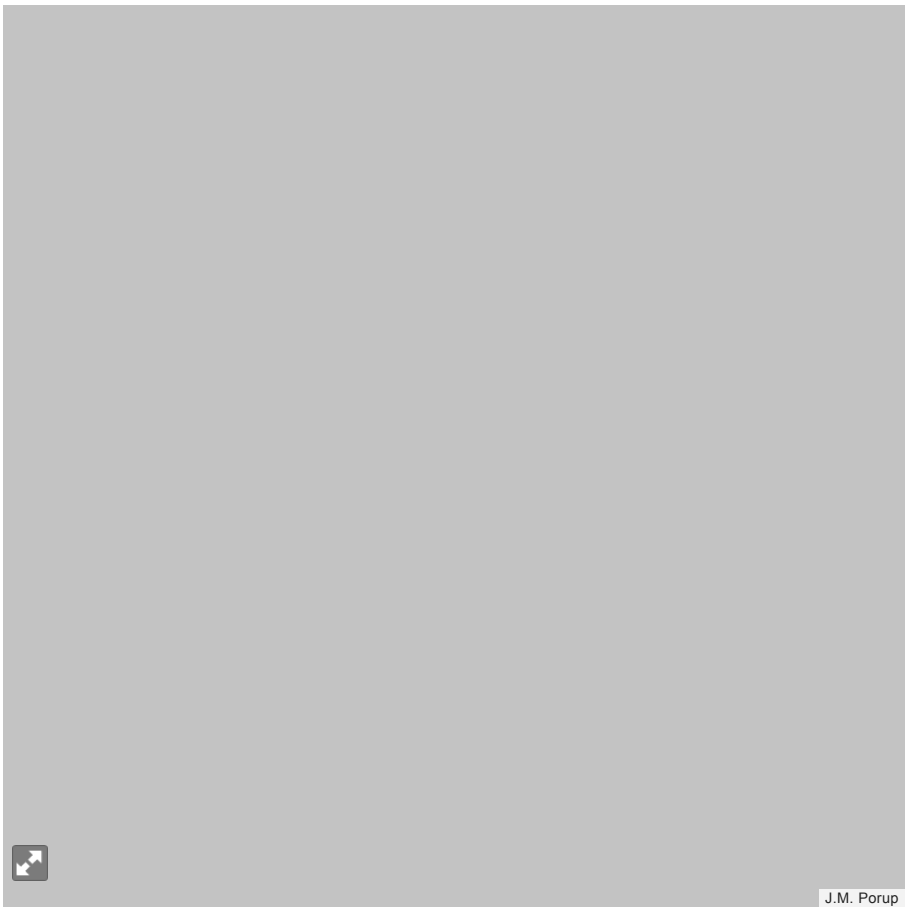
The `file` command tells us this isn't a valid PGP public key file. (Image modified to remove identifying information about our reporter's laptop.)



J.M. Porup

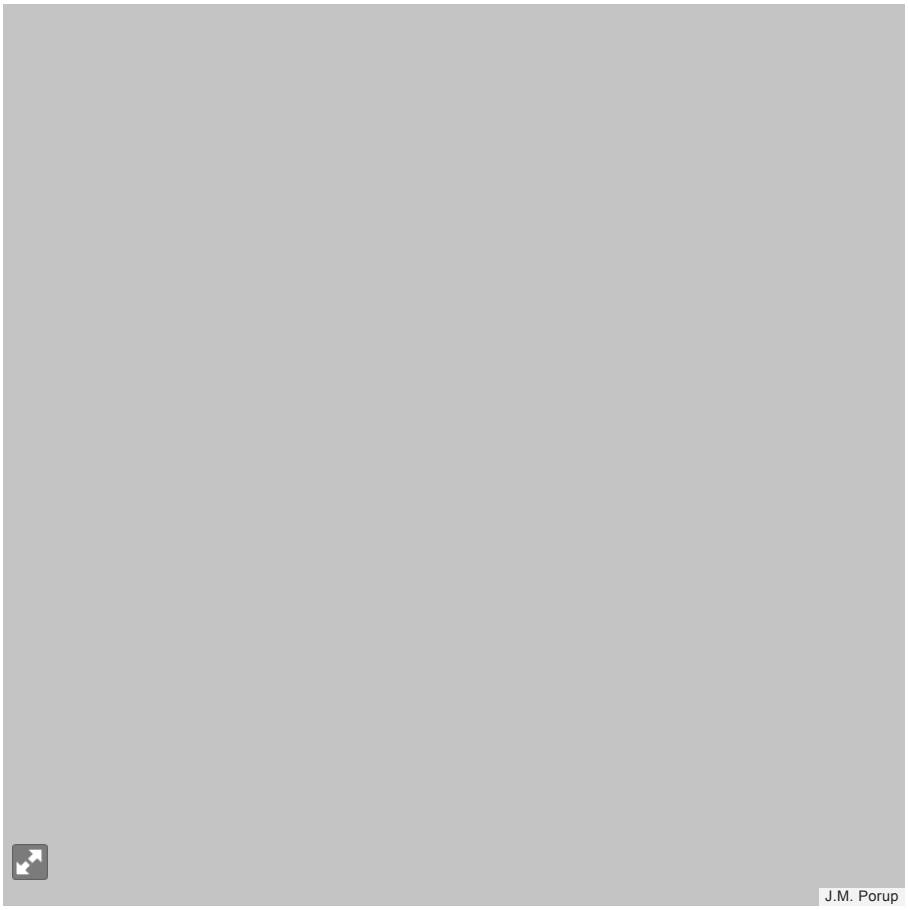
CSO attempted to import Boeing's new PGP public key to send them a test email, but the provided key is not a valid PGP

public key. (Image modified to remove identifying information about our reporter's laptop.)



Boeing's new PGP key, served over unencrypted HTTP. Security pros will note the lack of PGP headers in the public key file.

[Update November 8, 2019: As the screen image below shows, it appears that Boeing fixed the PGP issue on November 5, the day CSO *published this story.]*



J.M. Porup

Aviation and security research

The aviation industry is struggling to adapt to emerging cybersecurity issues, Beau Woods of security research advocacy group I Am the Cavalry tells *CSO*. "[Boeing] needs to understand that vulnerabilities aren't bad, per se, and that when someone reports one it's a good faith gesture and a teaching moment."

Kubecka emphasized in her talk at the Aviation Cyber Security Conference that Boeing is not an outlier in aviation when it comes to security and that she has uncovered gaping security lapses in every part of the aviation sector, including ticketing systems, air traffic control systems, and even gate jetway software. However, as one of the largest aircraft makers on the planet, security lapses at Boeing have the potential to affect passenger safety more than any other company in the space. She further alleges that their attempts to silence her good-faith research, an allegation that Boeing has denied, and the company's failure to remedy the security failures she reported demonstrate either an unwillingness or inability to take responsibility for their information security.

"Boeing’s internet facing infrastructure, web applications and email systems in general do not appear to have undergone basic to generally accepted security testing," Kubecka's vulnerability report concludes. Indeed, the company fully admits that the vulnerabilities Kubecka uncovered are remarkably common. "The security issues discussed in Ms. Kubecka’s report are, without exception, common IT vulnerabilities — the type of cyber-hygiene issues thousands of companies confront every day," the company told *CSO* in a statement.

The difference, of course, is that while poor cyber hygiene at Equifax might violate the privacy of Americans' credit histories, poor cyber hygiene at an aircraft manufacturer can possibly cause planes to fall out of the sky.

Software is eating the world, and today cybersecurity is the security of everything. Let's hope the aviation sector acts before it's too late.

More on critical infrastructure:

- **Critical Infrastructure Protection (CIP): Security problems exist despite compliance**
- **Is critical infrastructure the next DDoS target?**
- **Top IT security certifications for critical infrastructure — by sector**
- **Critical infrastructure: Off the web, out of danger?**

Next read this

- *8 cheap or free cybersecurity training resources*
- *12 tips for effectively presenting cybersecurity to the board*
- *24 best free security tools*
- *The new CISO's playbook: 5 rules to follow*
- *8 hot IT security jobs and what they pay*
- *5 steps to simple role-based access control*
- *11 top cloud security threats*
- *Top cyber security certifications: Who they're for, what they cost, and which you need*

Related: Critical Infrastructure | Security | Vulnerabilities

CSO senior security reporter J.M. Porup got his first job in IT security in 2002 as a Linux sysadmin. Got tips? jm_porup@idg.com

Follow

What 39 celebrities wore to meet the Queen
Marie Claire

[Photos] 33 Ads From The Past That Would Be Banned Today
The Primary Market

[Gallery] 20 Of The Most Decorated Military Heroes In U.S. History
Atlantic Mirror

What is application security? A process and tools for securing...
Homepage

4 authentication use cases: Which protocol to use?
Homepage

What is Security Onion? And can it replace your commercial IDS?
Homepage

Pregnant Dog Doesn't Want To Give Birth, Vet Does Ultrasound And Then Understands Why
Gloriousa

10 Credit Cards That Can't Be Beat In 2019
NerdWallet

Learn why a failure on the part of CIOs and CSOs to collaborate is putting companies at risk, because the necessary dialogue simply isn't happening.

Learn how Workplace by Facebook connects everyone in an organization using familiar tools like instant messaging, posts, and video calling.