DoD

(/dod/)

US Air Force moves to fortify F-35 weak points against hacking

By: Sebastian Sprenger (/author/sebastian-sprenger) November 14, 2018

BERLIN – The U.S. Air Force is devoting fresh energy to plugging cybersecurity holes in the F-35's external support systems, as they are deemed the easiest entry points for hackers into the fifth-generation combat jet, according to a key service official.

“It’s a software-based aircraft, and any software-based platform is going to be susceptible to hacking,” Brig. Gen. Stephen Jost, director of the Air Force F-35 Integration Office, told Defense News in an interview at the International Fighter industry conference here.

The service considers the information backbone of the actual airplane – managed by manufacturer Lockheed Martin – relatively safe. That is thanks to what Jost called “multilayer security protections” ranging from secure authentication when crafting mission data packages for each aircraft before takeoff, to pilots punching in personal identification numbers to start up the plane.

The confidence wanes “as you get further from the air vehicle,” Jost said. When taking into account systems like the Autonomic Logistics Information System or the Joint Reprogramming Environment, there are “a lot of nodes of vulnerability that we’re trying to shore up,” he added.

(https://www.defensenews.com/interviews/2018/11/12/pentagons-no-2-explains-his-lack-of-satisfaction-with-the-f-35/)

Patrick Shanahan on the F-35, modernization and budget cuts (https://www.defensenews.com/interviews/2018/11/12/pentagons-no-2-explains-his-lack-of-satisfaction-with-the-f-35/)

The deputy secretary of defense discusses his view on the budget, cutting costs and how to change the internal workings of the Pentagon.

By: Aaron Mehta

The Autonomic Logistics Information System, or ALIS, is a key application meant to provide unprecedented automation in monitoring the status of the aircraft's components. The Joint Reprogramming Enterprise refers to government software labs compiling collections of updated threat characteristics – Russian tanks, for example – for upload into the aircraft so that its sensors can recognize targets.

Additionally, officials worry about cyber-hardening F-35 flight simulators, which could be attractive targets for hackers seeking information about the plane. The introduction of wireless applications for easier maintenance on the flight line also could pose new vulnerabilities that must be addressed, Jost said.

The Government Accountability Office published a report in October warning warned about cyber vulnerabilities in almost all of the Defense Department's weapons. The shortfalls exist because many systems were conceived at a time when cyber attacks were still in their infancy.

“In operational testing, DOD routinely found mission-critical cyber vulnerabilities in systems that were under development, yet program officials GAO met with believed their systems were secure and discounted some test results as unrealistic,” auditors wrote. “Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications.”

A key examination phase for the F-35 program, called initial operational test and evaluation, was set to begin to this week. The test plan, required for all major programs, typically includes a regimen of cyber probing.

workforce-gap/)

from-cyberattacks/)

Around the Web

Comments

Most Watched Videos

▶ Play

How to stay anonymous for feds (Part 2) (/video/2018/11/16/how-to-stay-anonymous-for-feds-part-2/)

Lance Cottrell, chief scientist at Ntrepid, shows government workers how to remain anonymous online. (Daniel Woolfolk/Staff)
(/video/2018/11/16/how-to-stay-anonymous-for-feds-part-2/)

Estonia wants to shape world cyber laws on UN Security Council

▶ Play Video

(/video/2018/11/12/estonia-wants-to-shape-world-cyber-laws-on-un-security-council/)

A key factor to Estonia's cyber success (which the US has yet to replicate)

▶ Play Video

(/video/2018/11/05/a-key-factor-to-estonias-cyber-success-which-the-us-has-yet-to-replicate/)

Five Bits from Cybercon 2018

▶ Play Video

(/video/2018/11/02/five-bits-from-cybercon-2018/)

Top Headlines

Newsletters (http://link.fifthdomain.com/join/5ft/sign-up) Contact Us (/contact-us)

(https://www.linkedin.com/company/fifth-
(https://twitter.com/theFifthDomain2
(https://www.facebook.com/FifthDomain/)

Civilian (/civilian) DoD (/dod) Congress (/congress)
Critical Infrastructure (/critical-infrastructure) International (/international) Workforce (/workforce)
Industry (/industry) Thought Leadership (/thought-leadership)

Terms of Use
Terms of Service (http://sightlinemediagroup.com/terms-of-service/)
Privacy Policy (/privacy)
()
()

Get Us
Newsletters & Alerts (http://link.fifthdomain.com/join/5ft/sign-up)
RSS Feed (/rss)
()
()

Contact Us
Help & Contact Info (/contact-us)
Advertise (/advertising)
()
()

About Us
About Us (/about-us)
Careers (https://boards.greenhouse.io/sightlinemediagroup?gh_src=cpxe2a1)
()
()