Ethical hackers swarm Pentagon websites

05 MAR 2020 0

Government security, Security threats

Previous: Google launches FuzzB... Next: Facebook: No, we are not kil...

by Danny Bradbury

Hackers are crawling all over the US Department of Defense's websites. Don't worry, though: they're white hats, and DoD officials are quite happy about the whole thing.

Four years after it first invited white hat hackers to start hacking its systems, the Pentagon continues asking them to do their worst – and a report released this week says that they're submitting more vulnerability reports than ever.

The DoD's Department of Defense Cyber Crime Center (DC3) handles cybersecurity for the DoD, and is responsible for tasks including cyber technical training and vulnerability sharing. It also runs the DoD's Vulnerability Disclosure Program (VDP).

The VDP emerged from the Hack the Pentagon bug bounty program that the military ran in 2016. That initiative was so successful that it continues to invite hackers to play with its systems. Last year, the Air Force even bought an F-15 to Defcon for hackers to tinker with. Next year, it plans a satellite.

These high-profile events punctuate a more modest but ongoing program that invites hackers to submit security vulnerability reports focusing on DoD websites and web applications. The DoD engaged its DC3 unit to run the continuous program and keep the ethical hacks rolling in.

DC3 just published its first annual report on the program, revealing that it processed 4,013 vulnerability reports from 1,460 white hat researchers. It validated 2,836 of them for mitigation, it said, adding:

> *These vulnerabilities were previously unknown to the DoD and not found by automated network scanning software, red teams, manual configuration checks, or cyber inspections. Without DoD VDP there is a good chance those vulnerabilities would persist to this date, or worse, be active conduits for exploitation by our adversaries.*

2019 was the busiest year for bug reports, the report said, representing a 21.7% increase over 2017 and bringing the total number of bug reports to 12,489.

Information exposure bugs were the most common type reported during the year, followed by violation of secure design principles, cross-site scripting flaws, business logic errors, and open redirects (which are a way to mount phishing attacks).

In the future, DC3 wants to expand the scope of the program beyond DoD websites to cover any DoD information system. It also wants to partner with the Defense Counterintelligence and Security Agency (DCSA) to create what it calls a defense industrial base (DIB) VDP program to secure the DoD's supply chain. That's notable, given the past controversy over potential vulnerabilities in third-party drones and cameras sourced by the DoD.