GOVERNMENT

Ethical hackers submitted more bugs to the Pentagon than ever last year

(Defense Digital Service / Twitter)

Written by Shannon Vavra
Mar 2, 2020 | CYBERSCOOP

Outside security researchers alerted the Pentagon about more software vulnerabilities in its networks than ever before, according to statistics released by a Department of Defense unit focused on cyber operations.

The Defense Department's Cyber Crime Center (DC3) on Friday released its annual numbers from the Vulnerability Disclosure Program (VDP), in which the Pentagon asks ethical hackers,

It was our busiest year to date with a staggering 21.7% increase of submitted reports from 2017," the DOD Cyber Crime Center (DC3) report says.
The department has been working to uncover vulnerabilities with the help of white hat hackers for years. In 2016, the department launched "Hack the Pentagon" a program that rewarded white hat hackers who initially uncovered nearly 140 vulnerabilities in five public websites, for a payout of nearly $150,000. The Defense Department's willingness to adopt bug bounties in 2016, then an emerging concept, has been credited with moving this kind of security testing into the mainstream.

The director of the vulnerability disclosure program, Kristopher Johnson, said in February that many organizations remain reluctant to work with hackers, and that the Pentagon has gone through an internal transformation to partner with white hat hackers in the interest of bolstering government defenses. (Two years after the initial Hack the Pentagon program, the government announced it would spend $34 million to expand it.)

"Working with hackers to improve an organization's cyber hygiene was considered a revolutionary idea in 2016, but it has evolved to become almost commonplace in DOD," Johnson said in a blog post. "Trust is the foundation of the disclosure program…We trust that the hackers will follow the policy and do no harm."

What they found last year

Last year white hat hackers were particularly helpful in unveiling unpatched virtual private network (VPN) endpoints just as nation-state hackers latched onto exploiting vulnerabilities in VPN technologies to steal user credentials and monitor sensitive traffic. According to the report, these submissions from the program were the "most severe" findings from last year.
"VPN endpoints are not the only issue," the report notes. "We also see unpatched and exploitable content management servers such as DotNetNuke, WordPress, and even vBulletin with vulnerabilities ranging from simple reflected cross-site scripting and Denial of Service all the way to remote command execution."

The top two most common weaknesses that the vulnerability disclosures exposed last year included cases where DOD entities were exposing information to unauthorized outsiders, as well as violations of secure design principles. Cross-site scripting issues, business logic errors and open redirect flaws, which make it easier to carry out phishing attacks, also were among the top five weaknesses.

“

Other plans in the works

White hat hackers are already proving to be a valuable resource in uncovering vulnerabilities and weaknesses across the DOD this year, according to a January VDP assessment obtained by CyberScoop.

Violation of secure design principles topped the list of vulnerability types submitted last month, according to the assessment, with 139 reports highlighting secure design issues. Information disclosure issues, improper access control, operating system command injection issues, and cross-site scripting were the next most common.

Next, the VDP is working with both the Defense Counterintelligence and Security Agency (DCSA) and the DC3’s Defense Industrial Base Collaborative Information Sharing Environment (DCISE) to test a possible launch of a vulnerability disclosure program for the defense industrial base.

“We hope to replicate our success by leveraging both the DOD’s knowledge and capabilities for private defense companies that do not have the ability or resources to do this on their own,” the annual report says.

The assessment of a possible vulnerability disclosure program for the defense industrial base is scheduled to take nine months. It remains unclear what such a program might look like.