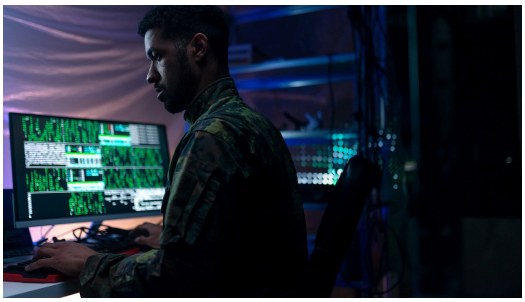
VULNERABILITIES

Pentagon Received Over 50,000 Vulnerability Reports Since 2016

Since 2016, the US DoD has received over 50,000 submissions through its vulnerability disclosure program.

By Ionut Arghire
March 18, 2024



The US Department of Defense on Friday announced that it has processed 50,000 reports received as part of its continuous

TRENDING

1 New Attack Shows Risks of Browsers Giving Websites Access to GPU
2 Cisco Completes $28 Billion Acquisition of Splunk
3 IMF Emails Hacked
4 Major CPU, Software Vendors Impacted by New GhostRace Attack

A first in the history of the federal government, the program was initiated following a successful 'Hack the Pentagon' bug bounty program running on HackerOne, which was followed by similar programs covering Air Force, Marine Corps, Army, and Defense Travel System assets.

Since then, the DoD ran over 40 bug bounty programs in collaboration with HackerOne, Bugcrowd, and Synack, and launched a continuous 'Hack the Pentagon' bug bounty program, allowing white hat hackers to submit vulnerability reports all-year-round.

By expanding the number of programs, DoD allowed security researchers to target a broader range of systems for bug hunting, ranging from high-value hardware and physical assets to web-facing websites and applications, HVAC, utilities, physical security systems, industrial control systems, and more.

In 2021, the DoD launched a 12-month bug bounty program aimed at finding flaws in contractor

7 43 Million Possibly Impacted by French Government Agency Data Breach

8 Nissan Data Breach Affects 100,000 Individuals

vulnerabilities, the Pentagon's Cyber Crime Center (DC3) says.

Last year, the DoD launched a Hack the Pentagon website to help DoD organizations establish their own bug bounty programs.

By the end of 2022, close to 45,000 vulnerability reports were received from roughly 4,000 researchers participating in the DoD's VDP. More than 25,000 of the reports were actionable and over 6,000 of them were successfully mitigated, the DoD said (PDF) last year.

According to the Pentagon's VDP page on HackerOne, more than 27,000 vulnerability reports have been resolved since the program's launch.

risk forcing users underground to use unknown tools with unknown consequences. (Alastair Paterson)

How Traffic, State, and Organizational Data Help Fortify Your Network

Traffic data is the lifeblood of network security, representing the raw, unfiltered truth of what is happening on the network. (Matt Wilson)

The Imperative for Modern Security: Risk-Based Vulnerability Management

By prioritizing vulnerabilities based on risk and aligning security efforts with business objectives, organizations can enhance their resilience to cyberattacks, optimize resource allocation, and maintain a proactive security posture. (Torsten George)

Is XDR Enough? The Hidden Gaps in Your Security Net

When evaluating XDR, consider its value based on its ability to reduce complexity and improve threat detection and response times. (Etay Maor)

Artificial Arms Race: What Can Automation and AI do to Advance Red Teams

The best Red Team engagements are a balanced mix of technology, tools and human operators. (Tom Eston)

ethical hacker community translates to the consistent strengthening of cyber defenses. As proud partners, we look forward to continued collaboration as ethical hackers work to further strengthen national security," HackerOne founder and CTO Alex Rice said.

Related: Lawmaker Wants Federal Contractors to Have Vulnerability Disclosure Policies

Related: US Defense Department Launches 'Hack the Pentagon' Website

Related: DoD Announces Final Results of 'Hack US' Bug Bounty Program

WRITTEN BY

Ionut Arghire

Ionut Arghire is an international correspondent for SecurityWeek.

More from Ionut Arghire

- Marketplace Sentenced to US Prison
- PoC Published for Critical Fortra Code Execution Vulnerability
- Codezero Raises $3.5 Million for DevOps Security Solution
- Discontinued Security Plugins Expose Many WordPress Sites to Takeover
- Tech Support Firms Agree to $26M FTC Settlement Over Fake Services
- Chrome's Standard Safe Browsing Now Has Real-Time URL Protection

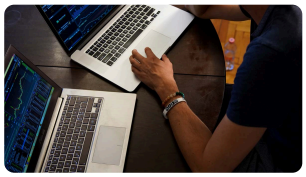
Latest News

- Aiohttp Vulnerability in Attacker Crosshairs
- UnitedHealth Says It Has Made Progress on Recovering From Massive Cyberattack
- UK Government Releases Cloud SCADA Security Guidance
- Fujitsu Data Breach Impacts Personal, Customer Information
- Cisco Completes $28 Billion Acquisition of Splunk
- Pentagon Received Over 50,000 Vulnerability Reports Since 2016
- Hacker Conversations: Stephanie 'Snow' Carruthers, Chief People Hacker at IBM X-Force Red
- New Attack Shows Risks of Browsers Giving Websites Access to GPU

Related Content

Full Disclosure List Gets a Fresh Start – Reborn Under New Operator

ChatGPT Data Breach Confirmed as Security Firm Warns of



16 Car Makers and Their Vehicles Hacked via Telematics,

Burglars Can Easily Disable SimpliSafe Alarms: Researcher

Cyber Insights 2023 | Supply Chain Security

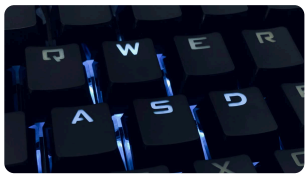
Kevin Townsend

Microsoft Warns of Office Zero-Day Attacks, No Patch Available

Ryan Naraine

Microsoft Warns of Outlook Zero-Day Exploitation, Patches 80 Security Vulns

Ryan Naraine



Chrome 111 Update Patches High-Severity Vulnerabilities

Ionut Arghire

Daily Briefing Newsletter

Subscribe to the SecurityWeek Daily Briefing and get the latest content delivered to your inbox.

Business Email Address...

Subscribe