MUST READ The Jailbreaking procedure is now legal in the United States

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | Laws and regulations | Malware | Mobile | Data Breach | Security | Social Networks | Reports | EXTENDED COOKIE POLICY | Contact me |

elligence Laws

XTENDED COOKIE PC

US Army Experts Call for military bug bounty program AVRP

October 28, 2015 By Pierluigi Paganini

G+1 1

My Page Like 6

US Army Military experts urge the establishment of an Army Vulnerability Response Program (AVRP), a sort of military bug bounty program.

What happen when bug hunters have to work with high *sensitive environment?*

An interesting post published by the Cyber Defense Review raises the discussion about the was to handle vulnerabilities in the information security infrastructure of the US Army. The post highlights the need of a Response Program for vulnerabilities affecting US army systems.

Current and former members of the department's cyber wing of the US Army, Captain Michael Weigand and Captain Rock Stevens, urge a joint project between the Army Cyber Institute and US Marine Corps Forces Cyberspace Command.

The military experts highlighted how essential aspects of the software lifecycle, like patch management and penetration testing are very difficult to carry on in these environments. The systems used in the US Army are exposed by an absence of centralized patch management and penetration testing are not allowed due to nature of the systems.

"Personnel who discover vulnerabilities encounter stumbling blocks from the first step of responsible disclosure–initial notification. If an employee does find the contact information for developer or program office, there is no external incentive or repercussion for a responsible pa to action the report or intelligence that is provided to them." states the post. "Additionally, it is possible that the report recipient could misinterpret the findings, not as valuable and friendly intelligence but rather as a threat to their contract, command, or system. Both scenarios yield t same result–the vulnerability remains and the report is dismissed. This wastes researcher's tim hard work, and promotes a "do-nothing" culture."

uld revoke them the security clearances, the access to IT systems, and face punitive action under the Uniform Code of Military Justice which they describe as "viable outcomes" for those who "casually stumble" on bugs.

"The most unfortunate outcome is that service members who become aware of vulnerabilities feel helpless to positively affect the situation. Meanwhile, those who wish to do harm to our nation are free from such worries," the experts added. *"Additionally, no US Government program exists that permits active security assessments of networks or software solutions using custom tools or techniques. Most importantly, the Army does not have a single entity that tracks discovered issues from initial report through the remediation process to ensure vulnerability resolution in a timely manner. Most of the Army's critical systems are underpinned by networked software — from tanks and missile launchers to battle command and communication systems. The Army does not have one central location for responsibly disclosing software vulnerabilities across all of its systems. Without a means to report vulnerabilities in Army software or networks, vulnerabilities go unreported and leave our information systems exposed to adversarial attacks."*

They call for a radical change, including the introduction of bug bounties, today internal experts who discovered vulnerabilities have no incentive to report the flaw are no obliged to disclose it, the post refers this bad habit as a "do nothing" culture.

MORE S

The Jail legal in

The Copy exemptic procedur the next.

Er

Pl it

In a paper published on the Cyber Defense Review website, the duo proposes the creation of an Army Vulnerability Response Program (AVRP), a bug bounty program run by the US military.

The Army Vulnerability Response Program (AVRP) platforms proposed by the military expert have to enable service people to report bugs free of risk of retribution, and say penetration tests should be promoted as vulnerability scans are inadequate.

> “
>
> *“The AVRP will serve as the central reporting mechanism for vulnerabilities in Army networks and will receive reports on poor configurations or gaps in security that could allow attackers to degrade Army systems. These systems include Army digital training management systems, Army Battle Command Systems, logistics procurement systems, and combat platforms deployed in hostile environments. Researchers can report vulnerabilities through a phone hotline or an online submission portal. The AVRP will track all submissions, facilitate the flow of*

communication with affected entities, and play an integral role in resolving the vulnerability throughout US government networks," the paper reads.

The AVRP project would be a closed program specifically designed for Department of Defense staff, but it is important also to involve externals although they would not be involved in the remediation process.

As an alternative to a bug bounty program completely managed by the US Army, the experts suggested using the services of specialized organizations such as Zero Day Initiative or Bugcrowd, but the costs would be high.

"If implementing an Army-run bug bounty program is not within the immediate goals/desire of any organization, there are third-party programs that can manage the program for the Army such as the Zero Day Initiative (ZDI) and Bug Crowd. Utilization of these third party programs would require a change to their current practices to handle classified disclosures which would most likely come at a substantial cost."

Pierluigi Paganini

(Security Affairs – Army Vulnerability Response Program (AVRP), bug bounty program)

Share it please ...

Share this:

Email | Twitter 13 | Print | LinkedIn 2 | Facebook 6 | More

AVRP | Bug Bounty | military bug bounty program AVRP | patch management | penetration testing | Security Affairs | US Army

Breaking News | Cyber warfare | Intelligence | Security

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

The Jailbreaking procedure is now legal in the United States

NEXT ARTICLE

Joomla SQL Injection Vulnerability exploited in the wild

YOU MIGHT ALSO LIKE

WhatsApp collects phone numbers, call duration, and a lot of metadata

October 27, 2015 By Pierluigi Paganini

TalkTalk CEO confirmed personally receiving a ransom demand

October 24, 2015 By Pierluigi Paganini