CERT Coordination Center

The **CERT Coordination Center** (**CERT/CC**) is the coordination center of the computer emergency response team (CERT) for the Software Engineering Institute (SEI), a non-profit United States federally funded research and development center. The CERT/CC researches software bugs that impact software and internet security, publishes research and information on its findings, and works with business and government to improve security of software and the internet as a whole.

CERT Coordination Center	
Type	FFRDC (part of Software Engineering Institute)
Industry	Software and Network Security
Founded	1988
Headquarters	Pittsburgh, PA, United States
Key people	US AF Brigadier General (ret) Gregory J. Touhill Director
Website	sei.cmu.edu/about/divisions/cert/index.cfm (http://sei.cmu.edu/about/divisions/cert/index.cfm)

History

The first organization of its kind, the CERT/CC was created in Pittsburgh in November 1988 at DARPA's direction in response to the Morris worm incident.[1] The CERT/CC is now part of the CERT Division of the Software Engineering Institute, which has more than 150 cybersecurity professionals working on projects that take a proactive approach to securing systems. The CERT Program partners with government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats.

The CERT Program is part of the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) at Carnegie Mellon University's main campus in Pittsburgh. CERT is a registered trademark of Carnegie Mellon University.[2]

Confusion with US-CERT and other CERTs

In 2003, the Department of Homeland Security entered into an agreement with Carnegie Mellon University to create US-CERT.[3] US-CERT is the national computer security incident response team (CSIRT) for the United States of America. This cooperation often causes confusion between the CERT/CC and US-CERT. While related, the two organizations are distinct entities. In

general, US-CERT handles cases that concern US national security, whereas CERT/CC handles more general cases, often internationally.

The CERT/CC coordinates information with US-CERT and other computer security incident response teams, some of which are licensed to use the name “CERT.” [4] While these organizations license the "CERT" name from Carnegie Mellon University, these organizations are independent entities established in their own countries and are not operated by the CERT/CC.

The CERT/CC established FIRST, an organization promoting cooperating and information exchange between the various National CERTs and private Product Security PSIRTs.

Capabilities

The research work of the CERT/CC is split up into several different Work Areas.[5] Some key capabilities and products are listed below.

Coordination

The CERT/CC works directly with software vendors in the private sector as well as government agencies to address software vulnerabilities and provide fixes to the public. This process is known as coordination.

The CERT/CC promotes a particular process of coordination known as *Responsible Coordinated Disclosure*. In this case, the CERT/CC works privately with the vendor to address the vulnerability before a public report is published, usually jointly with the vendor's own security advisory. In extreme cases when the vendor is unwilling to resolve the issue or cannot be contacted, the CERT/CC typically discloses information publicly after 45 days since first contact attempt.[6]

Software vulnerabilities coordinated by the CERT/CC may come from internal research or from outside reporting. Vulnerabilities discovered by outside individuals or organizations may be reported to the CERT/CC using the CERT/CC's Vulnerability Reporting Form.[7] Depending on severity of the reported vulnerability, the CERT/CC may take further action to address the vulnerability and coordinate with the software vendor.

Knowledge Base and Vulnerability Notes

The CERT/CC regularly publishes Vulnerability Notes in the CERT KnowledgeBase.[8][9] Vulnerability Notes include information about recent vulnerabilities that were researched and coordinated, and how individuals and organizations may mitigate such vulnerabilities.

The Vulnerability Notes database is not meant to be comprehensive.

Vulnerability Analysis Tools

The CERT/CC provides a number of free tools to the security research community.[10] Some tools offered include the following.

- CERT Tapioca—a pre-configured virtual appliance for performing man-in-the-middle attacks. This can be used to analyze network traffic of software applications and determine if the software uses encryption correctly, etc.
- BFF (Basic Fuzzer Framework)—a mutational file fuzzer for Linux
- FOE (Failure Observation Engine)—a mutational file fuzzer for Windows
- Dranzer—Microsoft ActiveX vulnerability discovery

Training

The CERT/CC periodically offers training courses for researchers, or organizations looking to establish their own PSIRTs.[11]

CERT Coordination Center

Controversies

In the summer of 2014, CERT research funded by the US Federal Government was key to the de-anonymization of Tor, and information subpoenaed from CERT by the FBI was used to take down SilkRoad 2.0 that fall. FBI denied paying CMU to deanonymize users,[12] and CMU denied receiving funding for its compliance with the government's subpoena.[13]

Despite indirectly contributing to taking down numerous illicit websites and the arrest of at least 17 suspects, the research raised multiple issues:

- about computer security research ethics as a concern to the Tor community[14] and others[15]

- about being unreasonably searched online as related to the guarantee by the US 4th amendment[14]
- about SEI/CERT acting at cross-purposes to its own missions, actions including withholding the vulnerabilities it had found from the software implementers and the public.[15]

CMU said in a statement in November 2015 that "...the university from time to time is served with subpoenas requesting information about research it has performed. The university abides by the rule of law, complies with lawfully issued subpoenas and receives no funding for its compliance", even though Motherboard reported that neither the FBI nor CMU explained how the authority first learned about the research and then subpoenaed for the appropriate information.[13] In the past, SEI had also declined to explain the nature of this particular research in response to press inquiries saying: "Thanks for your inquiry, but it is our practice not to comment on law enforcement investigations or court proceedings."[16]

See also

- CERT C Coding Standard
- Computer Emergency Response Team
- Computer security

References

1. *"About Us: The CERT Division" (http://cert.org/about/)* . *Software Engineering Institute. Carnegie Mellon University. Retrieved March 9, 2015.*
2. *"Trademarks and Service Marks" (http://www.sei.cmu.edu/legal/marks/)* . *Software Engineering Institute. Carnegie Mellon University. Retrieved December 7, 2014.*
3. *"U.S. Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center" (http://www.sei.cmu.edu/newsitems/uscert.cfm)* . *SEI Press Release. Carnegie Mellon University. September 15, 2003. Retrieved December 7, 2014.*
4. *"National CSIRTs" (http://cert.org/incident-management/national-csirts/index.cfm)* . *Carnegie Mellon University. Retrieved March 9, 2015.*
5. *CERT/CC. "The CERT Division" (http://cert.org/)* . *Retrieved March 9, 2015.*
6. *"Vulnerability Disclosure Policy" (http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm?)* . *Software Engineering Institute. Carnegie Mellon University. Retrieved March 9, 2015.*
7. *"CERT Coordination Center" (https://forms.cert.org/VulReport/)* .

8. *"Vulnerability Notes Database" (http://www.kb.cert.org/vuls/)* . *Software Engineering Institute. Carnegie Mellon University. Retrieved October 27, 2017.*
9. *Cory Bennett (November 3, 2014). "New initiative aims to fix software security flaws" (http://thehill.com/policy/cybersecurity/222639-new-initiative-aims-to-fix-software-security-flaws)* . *TheHill. Retrieved December 6, 2014.*
10. *"Vulnerability Analysis Tools" (http://www.cert.org/vulnerability-analysis/tools/index.cfm)* . *Software Engineering Institute. Carnegie Mellon University. Retrieved March 9, 2015.*
11. *"CERT Training Courses" (http://www.cert.org/training/)* . *Software Engineering Institute. Carnegie Mellon University. Retrieved March 9, 2015.*
12. *"FBI: 'The allegation that we paid CMU $1M to hack into Tor is inaccurate'" (https://arstechnica.com/tech-policy/2015/11/fbi-the-allegation-that-we-paid-cmu-1m-to-hack-into-tor-is-inaccurate/)* . *Ars Technica. November 14, 2015.*
13. *"US defence department funded Carnegie Mellon research to break Tor" (https://www.theguardian.com/technology/2016/feb/25/us-defence-department-funding-carnegie-mellon-research-break-tor)* . *The Guardian. February 25, 2016.*
14. *Dingledine, Roger (November 11, 2015). "Did the FBI Pay a University to Attack Tor Users?" (https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users)* . *Tor Project. Retrieved November 20, 2015.*
15. *Felten, Ed (July 31, 2014). "Why were CERT researchers attacking Tor?" (https://freedom-to-tinker.com/blog/felten/why-were-cert-researchers-attacking-tor/)* . *Freedom to Tinker, Center for Information Technology Policy, Princeton University.*
16. *"Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects" (http://motherboard.vice.com/read/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects)* . *Motherboard. November 11, 2015. Retrieved November 20, 2015.*

External links

- Official website (https://www.sei.cmu.edu/about/divisions/cert/index.cfm)

title=CERT_Coordination_Center&oldid=1074546779"

Last edited 5 months ago **by** Nacho319