CENSUS
IT Security Works

VULNERABILITY RESEARCH

A vulnerability is a state in a computing system that violates the system's security model. As a leader in IT Security services CENSUS heavily invests in vulnerability research to identify and expose unknown vulnerabilities in today's computing systems. Now, through the Vulnerability Research services, CENSUS makes its research team available to organizations, enabling them to investigate in depth the security of protocols, technologies and products.

HOW IS VULNERABILITY RESEARCH DIFFERENT FROM A PENETRATION TEST?

A penetration test examines if security controls are effective in protecting a particular asset in a particular setup. Vulnerability research considers the protocol / technology / product itself as the asset and searches for exploitable vulnerabilities in the asset. In this way, one may measure the level of risk involved in introducing the investigated technology into a system or infrastructure.

HOW DOES IT COMPARE TO CODE AUDITING?

Vulnerability research allows the identification of exploitable security bugs in software where the source code may not be available. Also, it is a more elaborate process than Code Auditing, as the mechanics of exploiting each defect are analyzed in depth and the implications of each defect are studied per different systems / environments. The type of knowledge acquired through vulnerability research services is sometimes referred to as security intelligence.

METHODOLOGY

CENSUS employs a top-down approach to vulnerability research, that enables the quick identification of components that are exposed to security threats. Exposed components are examined for vulnerabilities using a variety of focused techniques including Fuzzing, Source Code Auditing (in cases where source code is available), Reverse Engineering and advanced Program Analysis. Protocol Analysis methods are also used to identify issues in the design of communication or other protocols.
The exploitable nature of each identified vulnerability is demonstrated and analyzed using proof-of-concept code and the impact of exploitation is studied across different systems and environments.

FUZZING

Fuzz Testing, or Fuzzing, is a technique in which the inputs of the investigated IT system are identified and purposefully built invalid, unexpected and random data are provided to them. All triggered failures of the system are recorded and subsequently analyzed to uncover possible security implications. Smart Fuzzing allows the probing of systems in both depth and width while taking under consideration the time limitations inherent to each project.

SOURCE CODE AUDITING

When source code is available, Source Code Auditing allows for the potential uncovering of all vulnerabilities in a piece of software. Here, the identification of exploitable security flaws occurs through a line-by-line analysis of the source code of the target application / protocol implementation.

REVERSE ENGINEERING

When source code is not available, reverse engineering techniques are employed to uncover exploitable security defects. The target implementation is disassembled and its raw machine code is studied to uncover both logic and implementation vulnerabilities. Reverse Engineering can employ Static and Dynamic Analysis techniques; in the first case the disassembled code is processed line-by-line while in the second case it is analyzed while the system is running.

PROGRAM ANALYSIS

Advanced Program Analysis processes assist the manual examination of large code bases during vulnerability research. To reap the full benefits of Program Analysis methods, CENSUS employs both static and dynamic Program Analysis technologies. These technologies play a crucial role in revealing interesting components and code paths that will later be investigated through manual auditing by researchers. The result is increased efficiency and significant time gains in the identification of security bugs.

PROTOCOL ANALYSIS

Protocol Analysis methods allow for the identification of security issues that are inherent to the design of a particular protocol. Using the information that is available about the protocol states, researchers examine whether an implementation of the protocol would be subject to man-in-the-middle, replay, spoofing and other attacks.

DELIVERABLES

Depending on the type of assessment, a detailed technical report with the research findings can be delivered either at the end of the assessment or at each research milestone. The report contains:

- An executive summary
- A detailed description of the research conducted and its findings
- An evaluation of the exploitation possibilities for each finding and the related risks
- Proof-of-concept code for each exploitable issue
- Optionally, a threat model for the investigated technology

BENEFITS

Vulnerability Research enables:

- The preemptive reduction of risks associated with the investigated technology
- Informed decision making based on risk evaluation
- The collection of key security intelligence information
- The empowerment of R&D teams through the delivery of key insights

For more information about the Vulnerability Research services offered by CENSUS please visit http://census-labs.com

CENSUS
IT Security Works

Stadiou 33, 10559,
Athens, Greece
T. +30 2110 128 355
F. +30 2310 947 234

I. Gkoura 16, 54352,
Thessaloniki, Greece
T. +30 2310 947 233
F. +30 2310 947 234

E. info@census-labs.com
www.census-labs.com