

census[®]

Vulnerability Research



A vulnerability is a state in a computing system that violates that system's security model. At Census we recognise that security is not a goal but a process. Therefore we heavily invest in research for unknown vulnerabilities as part of our security assessment services. The Census Vulnerability Research service enables our clients to preemptively reduce risk and protect the ROI of their IT assets by exposing their security flaws.

A client can use our Vulnerability Research services in order to ensure that a software product, a system implementation, or a new technology he is planning to invest in meets strict security requirements and does not suffer from vulnerabilities. Census can provide detailed deliverables that empower the client to make informed strategic decisions towards new technologies, choose the most secure solution that meets his requirements, and preemptively reduce investment risk.

Methodology

Census employs a top-down approach which allows for the identification of the most exposed elements of the investigated system. We then perform a thorough investigation for unknown vulnerabilities in these elements. We have extensive experience and specialized knowledge in the field of vulnerability research and we employ focused techniques such as Fuzzing, Source Code Auditing (in cases where source code is available), Reverse Engineering, Static and Dynamic Analysis in order to identify software vulnerabilities and clearly demonstrate their impact on a system's security model.

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 us to probe systems in both depth and width while taking under consideration the time limitation requirements of the client.

Source Code Auditing

Source Code Auditing is the most detailed step of the Vulnerability Research methodology with the potential to uncover the maximum number of vulnerabilities. Source Code Auditing is conducted in cases where the target system's source code is available and there is a sufficient project time frame. Census investigates the complete source code of the target application (web-based or standalone) on a line-by-line basis for security flaws that can enable an attacker to take control of the application or gain access to the underlying system that hosts the application. Census can provide Source Code Auditing services for software implemented in the following languages: C, C++, Java, C#, PHP, Python, Perl, ASP, Visual Basic.

Reverse Engineering

In cases where there is no source code available for a target system, the Census Vulnerability Research methodology employs Reverse Engineering techniques in order to uncover security flaws. The target system 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 read line-by-line while in the second one it is analyzed while the system runs (under normal use and under stress conditions, for example under Fuzzing).

census[®]

census[®]

Vulnerability Research

Deliverables

- An immediate report in the case that an uncovered security flaw threatens business viability and continuity.
- An executive summary report with a high level description of the performed research and the findings.
- A detailed technical report describing the performed research and the recommended corrective steps.
- A threat modeling report that presents the attack paths enabling the client to understand and benchmark their real security level.
- A risk assessment report for the scope of the project, enabling clients to plan their security management policy and incorporate in it the results of the Vulnerability Research service. Census can also provide continuing services to ensure an on-budget / on-time implementation of such a policy.

Benefits

The Census Vulnerability Research service offers a number of key benefits.

Preemptive Reduction of Security Risk

The Census Vulnerability Research service offers clients the opportunity to stay protected against possible future attacks through discovered security flaws in their IT assets. The client is given the advantage to mitigate the discovered vulnerabilities before they are exploited by potential malicious attackers. Security risk is reduced and the critical business information and intellectual property of the client is preemptively protected.

Protection of the ROI of IT assets

Information Technology assets (such as databases, ERP systems, web applications, custom developed software and systems, etc.) represent investments that a client is expecting ROI from. Successful attacks against these assets compromise the client's means of revenue generation, not to mention the incalculable damage to their market reputation. Census enables its clients to protect the ROI of their IT assets by exposing their security flaws.

Enable Informed Decision Making and Protect Investments

By utilizing the Census Vulnerability Research service and the deliverables that Census provides, clients are enabled to make informed investment decisions. By ensuring that a new technology, software product or IT system meets strict security requirements and does not suffer from vulnerabilities, the client's investment is protected.

census[®]

