

Study finds seven out of ten retail and finance applications vulnerable to Heartbleed-style attacks

CAST determines retail and finance applications are most vulnerable to input validation attacks if software risk goes unaddressed

August 27, 2014 - New York/London - CAST, a leader in software analysis and measurement, today revealed new findings from its ongoing research on application software health that confirms the growing number of data breaches and security incidents can be directly linked to poor [code quality](#). The data reveals finance and retail industry applications are the most vulnerable to data breaches, with 70 percent of retail and 69 percent of financial services applications shown to have data input validation violations. This is particularly concerning, considering the amount of personal and financial customer data often held in applications across these industries.

CAST EVP Lev Lesokhin who led the security analysis said, "So long as IT organizations sacrifice software quality and security for the sake of meeting unrealistic schedules, we can expect to see more high-profile attacks leading to the exposure and exploitation of sensitive customer data. Businesses handling customer financial information have a responsibility to improve software quality and reduce the operational risk of their applications -- not only to protect their businesses, but ultimately their customers."

Input validation has gotten a great deal of attention this year thanks to the Heartbleed bug, which exposed over 60 percent of the internet's servers to intrusion due to improper input validation in the form of a missing bounds check in the implementation of the TLS heartbeat extension. As of June, 21 2014, it's estimated that [309,197 public web servers](#) still remained vulnerable. In addition, [a recent report revealed](#) that input validation attacks were exploited in 80 percent of attacks against applications last year in the retail industry alone -- with perhaps the largest casualty being the record breaking eBay data breach, resulting in hackers gaining access to over 145 million user records and a federal investigation.

CAST also found that -- contrary to public perception -- government IT had the highest percentage of applications without any input validation violations (61 percent), while independent software vendors came in dead last (12 percent without violations). Even more surprising, the data showed that the financial services industry has the highest number of input validation violations per application (224) even though their applications, on average, are only half as complex as the largest application scanned.

In its biennial CRASH Report on the global state of quality in business applications to be released in September, CAST found a significant correlation between application robustness, its ability to avoid failures, and application security. Dr. Bill Curtis, chief scientist at CAST and author of the CRASH Report, said, "Some security experts argue software security is different from software quality and should be treated separately. The CRASH Report

data proves this is false. Badly-constructed software won't just cause systems to crash, corrupt data, and make recovery difficult, but also leaves numerous security holes.”

About CAST

CAST is a pioneer and world leader in software analysis and measurement, with unique technology resulting from \$120 million in R&D investment. CAST introduces fact-based transparency into application development and sourcing to transform it into a management discipline. More than 250 companies across all industry sectors and geographies rely on CAST to prevent business disruption while reducing hard IT costs and software risk. CAST is an integral part of software delivery and maintenance at the world's leading IT service providers. Founded in 1990, CAST is listed on NYSE-Euronext (Euronext: CAS) and serves IT intensive enterprises worldwide with offices in North America, Europe and India.

For more information about CAST:

Web: <http://www.castsoftware.com>

Blog: <http://blog.castsoftware.com>

Twitter: <http://www.twitter.com/onquality>

PR Contact:

Tara Szalkowski

communications@castsoftware.com

+1-212-871-8335