Application Vulnerability Assessment Process

Scope of Assessment

Digital Insight commissions independent security firms to perform application vulnerability assessments of all deployed consumer and commercial offerings. The primary goal is to identify vulnerabilities that might permit unauthorized access to confidential data, unauthorized transactions, or service disruption.

Summary of Approach

Planning and execution occur over a period of two to four weeks, and vulnerability testing is conducted over roughly a two or three-week period. The vulnerability assessment focuses on flaws that would allow unauthorized access to confidential data and sensitive functions, or access to underlying servers, including web application flaws which allow for hijacking of user sessions and altering customer data. Examples of vulnerabilities tested for include, but are not limited to:

- Application Exception
- Authorization Bypass
- Blind SQL Injection
- Buffer Overflow
- Cookie Security
- Credit Card Disclosure
- Cross Frame Scripting
- Cross Site Request Forgery
- Cross-Site Scripting
- CSV injection
- Denial of Service
- Direct Object Reference
- Directory Browsing
- Document Caching
- File and Directory Discovery
- Form Caching
- Format String
- HTTP Response Splitting
- O/S Command Injection
- Password Autocomplete
- Privilege Escalation
- Session Fixation
- Session Hijacking
- SSL bypass
- Unencrypted storage on device
- Weak Password
- Web Server Configuration
- Windows/Unix Relative Path

Assessment results are promptly reviewed to identify false positives and to prioritize relevant risk items for attention by area managers. All risks identified are tracked by management to final disposition.

Revised February 15, 2018

Ongoing Security Oversight

It is important to note, that, in addition to the independent application vulnerability assessment process described by this document, technical risk assessments are performed by Digital Insight ongoing as a formal part of the System Development Life Cycle process. Specifically, as changes are made to deployed applications, security oversight is applied to the design, code, and test phases of the development lifecycle to ensure that new risks are not introduced into the production environment. Both automated tools and manual review are employed to ensure that risks are identified prior to deployment.

Further, if it is determined that substantial changes are required to application or infrastructure, or if the threat environment changes substantially, a complete independent application vulnerability assessment will be performed at that time.