ccTLD Security Assessments

Cynthia Kern, Principal Program Manager

Nick Whitworth, Domains Business Manager

April 8th, 2013

Microsoft®

Current Trends

ccTLDs are at Risk

- The exploitation of vulnerabilities specific to country-code top-level domain (ccTLD) registries has become an **increasingly common problem**, especially in relatively small markets around the world

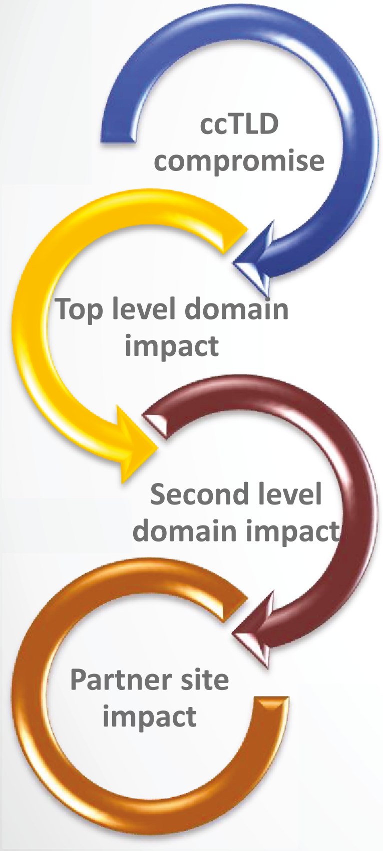
- Attacks on ccTLDs have **far-reaching effects** on private individuals, large and small companies, non-profits, and government organizations

- Attacking a TLD is a way for hackers **to impact a large number of organizations** and **gain notoriety**, making ccTLDs an attractive target

Approximately 12 TLDs successfully hacked since November 2012

Online Community Impact

What can Happen



- **Wide-spread impact** of compromised ccTLD registries result in unavailable sites and lost revenue

- Risk of **downstream site compromise** – malicious manipulation of the Domain Name System (DNS) records, specific to individual country markets has an adverse impact on the global online community

- Redirection of customers, collection of customer credentials **impact business reputation** in the online marketplace

Security Assessment

Prevention is the Best Defense

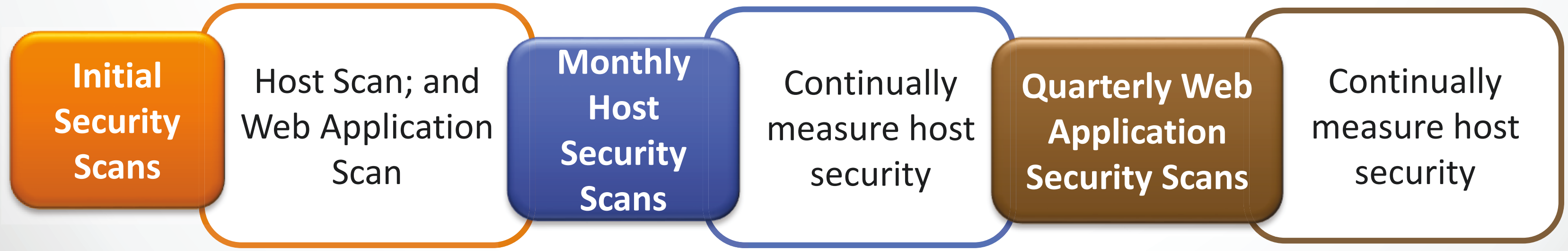
- **Identifying risk before it is discovered** by external parties is key to protecting ccTLD registries (i.e. Cross-site scripting, SQL injection and cross-site request forgery)
- Microsoft Country-Code Top-Level Domain (ccTLD) Registry Security Assessment Service is **designed to help registry operators find and fix security vulnerabilities before they are exploited** by leveraging scanning tools to identify weaknesses
- **Best practice collateral and security advisory** are also included to help educate ccTLD operators with security vulnerability remediation
- Microsoft is providing this service **free of charge** to ccTLD Registry operators to promote security at a global level

Security Assessment Process

To Get Started

- Send an email to ccTLDRegSec@microsoft.com that provides:
  - Requestor name and email contact
  - Approval name and email contact for scanning authorization
  - IP(s) and URL(s) for Public Facing Portals for Registrars

- IP(s) and URL(s) provided by the ccTLD will be scanned and results provided within 7 days



Initial Security Scans

Host Scan; and Web Application Scan

Monthly Host Security Scans

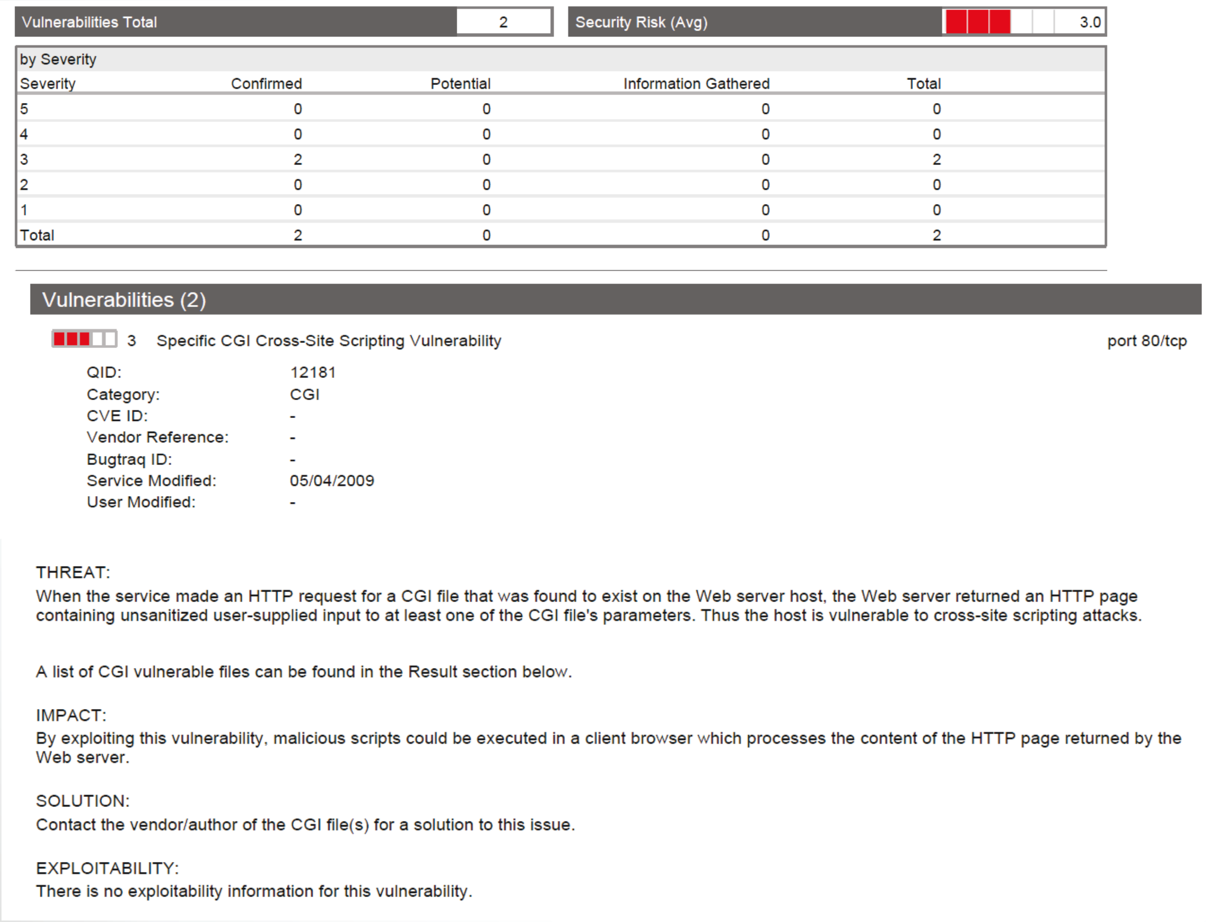
Continually measure host security

Quarterly Web Application Security Scans

Continually measure host security

Security Reports

When Vulnerabilities are Identified



Vulnerabilities Total	2	Security Risk (Avg)	🟥🟥🟥⬜⬜ 3.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	2	0	0	2
2	0	0	0	0
1	0	0	0	0
Total	2	0	0	2

Vulnerabilities (2)

🟥🟥🟥⬜⬜ 3 Specific CGI Cross-Site Scripting Vulnerability port 80/tcp

QID:	12181
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2009
User Modified:	-

THREAT:
When the service made an HTTP request for a CGI file that was found to exist on the Web server host, the Web server returned an HTTP page containing unsanitized user-supplied input to at least one of the CGI file's parameters. Thus the host is vulnerable to cross-site scripting attacks.

A list of CGI vulnerable files can be found in the Result section below.

IMPACT:
By exploiting this vulnerability, malicious scripts could be executed in a client browser which processes the content of the HTTP page returned by the Web server.

SOLUTION:
Contact the vendor/author of the CGI file(s) for a solution to this issue.

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

Far Reaching Benefit

Creating a Secure Online Experience

- Maintaining security at the ccTLD registry level **benefits everyone** – businesses and their customers

- Security in the online environment is a **shared responsibility**

- Leveraging the Microsoft Country-Code Top-Level Domain (ccTLD) Registry Security Assessment Service is a simple way to **get started in measuring your ccTLD host and web application security**

Microsoft ccTLD Security Assessment Service

To learn more about this service:

ccTLD Service Announcement
ccTLD Service Advisory Page
Terms of Use
cctldregsec@microsoft.com

Microsoft®

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.