IBM Security Systems  Technical Update

X-Force Q3 2014 Report :

Domenico Raguseo, Europe Technical Sales Manager
dom.ragueo@it.ibm.com
Linkedin : http://it.linkedin.com/in/draguseo
Twitter  : @domenicolraguseo
Facebook : https://www.facebook.com/draguseo

October 2014
Expert analysis and data sharing on the global threat landscape

The IBM X-Force Mission
- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow’s security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter
X-Force is the foundation for advanced security and threat research across the IBM Security Framework

The mission of X-Force is to:

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow’s security challenges
- **Educate** our customers and the general public
X-Force has the skills and infrastructure necessary for collecting & analyzing these changing threats.

**Internet**

**Global Data Center**
- Over 15 years of experience
- Over 20 Billion pages and addresses catalogued
- Databases dynamically updated on a minute-by-minute basis

**Data capture**
- Crawler robots search the web in parallel
- Honeypots & darknets capture information
- Spamtraps obtain Spam IPs and samples

**Threat Intelligence Databases**

**Analysis**
- Server clusters analyze the data acquired
- Insights for different threats are gleaned from the data and stored in an efficient manner

**Online Services**
IBM X-Force – Protecting against the vulnerability, not the exploit

<table>
<thead>
<tr>
<th>X-Force focuses on vulnerabilities and exploitation methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deep Protocol Analysis</strong></td>
</tr>
<tr>
<td>Full network protocol, application, and content analysis parsers.</td>
</tr>
<tr>
<td><strong>Vulnerability Decodes</strong></td>
</tr>
<tr>
<td>Knowing what 'normal' looks like allows for accurate inspection, reliable performance, and accurate detection of attack conditions.</td>
</tr>
<tr>
<td><strong>Shellcode Detection</strong></td>
</tr>
<tr>
<td>We research what methods can be used to reliably exploit, bypass protection and blend into the background.</td>
</tr>
</tbody>
</table>

The Exploit

- **Normal Data**
  - Get to vulnerable section of code

- **Malformed Data**
  - Triggers the vulnerability

- **Remote Shell**
  - Payload to gain remote access

**Vulnerable Code**

© 2014 IBM Corporation
More than half a billion records of personally identifiable information (PII) were leaked in 2013.

Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation
The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.
OpenSSL heartbeat information disclosure openssl-cve20140160-info-disc (92322) **High Risk**

**Description:**
OpenSSL could allow a remote attacker to obtain sensitive information, caused by an error in the TLS/DTLS heartbeat functionality. An attacker could exploit this vulnerability to expose 64k of private memory and retrieve secret keys.
Heartbleed attack activity for IBM Managed Security Services customers

April 2014

Attacks peaked with more than 300,000 attacks in one day

Figure 1. Attack activity related to the Heartbleed vulnerability, as noted for IBM Managed Security Services customers, in April 2014
Sampling of Heartbleed attack activity
24 April 2014 through 1 July 2014

Final peak in distributed attacks

Attack activity still averages 7,000 per day

Figure 3. Sampling of Heartbleed attack activity for IBM Managed Security Services customers, 24 April 2014 through 1 July 2014

© 2014 IBM Corporation
The Race to prevent one day attack

Timeline of one-day attacks for Heartbleed vulnerability
7 April 2014 through 9 April 2014

2014

7 April 2014
Heartbleed security advisory issued (CVE-2014-0160)

8 April 2014
First proof-of-concept began circulating
Attack against a Mandiant client occurred
Canadian Revenue Agency removed public access to its online services, but a breach had already occurred

9 April 2014
Mumsnet patched its systems, but a breach had already occurred

Figure 4. Timeline of one-day attacks for Heartbleed vulnerability (CVE-2014-0160), 7 April 2014 through 9 April 2014
Vulnerability disclosures in the first half of 2014

Figure 6. Vulnerability disclosures growth by year, 1996 through 2014 (projected)
At first glance, the recent announcement of a new vulnerability (classified on the National Vulnerability Database as CVE 2014-6271) in the Bash shell might not seem like a big deal. The vulnerability, nicknamed "Shellshock," is remotely exploitable under the right conditions and affects the Bash shell versions 1.14 through 4.3, which means that it has been around for more than 20 years.

Simple Test:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"

vulnerable
this is a test
```

IBM has been helping to protect customers from this and similar attacks since 2007, thanks to Protocol Analysis with Shell_Command_Injection signature of our Network Intrusion Prevention System.