# Security Now! #459 - 06-10-14
# Q&A #189

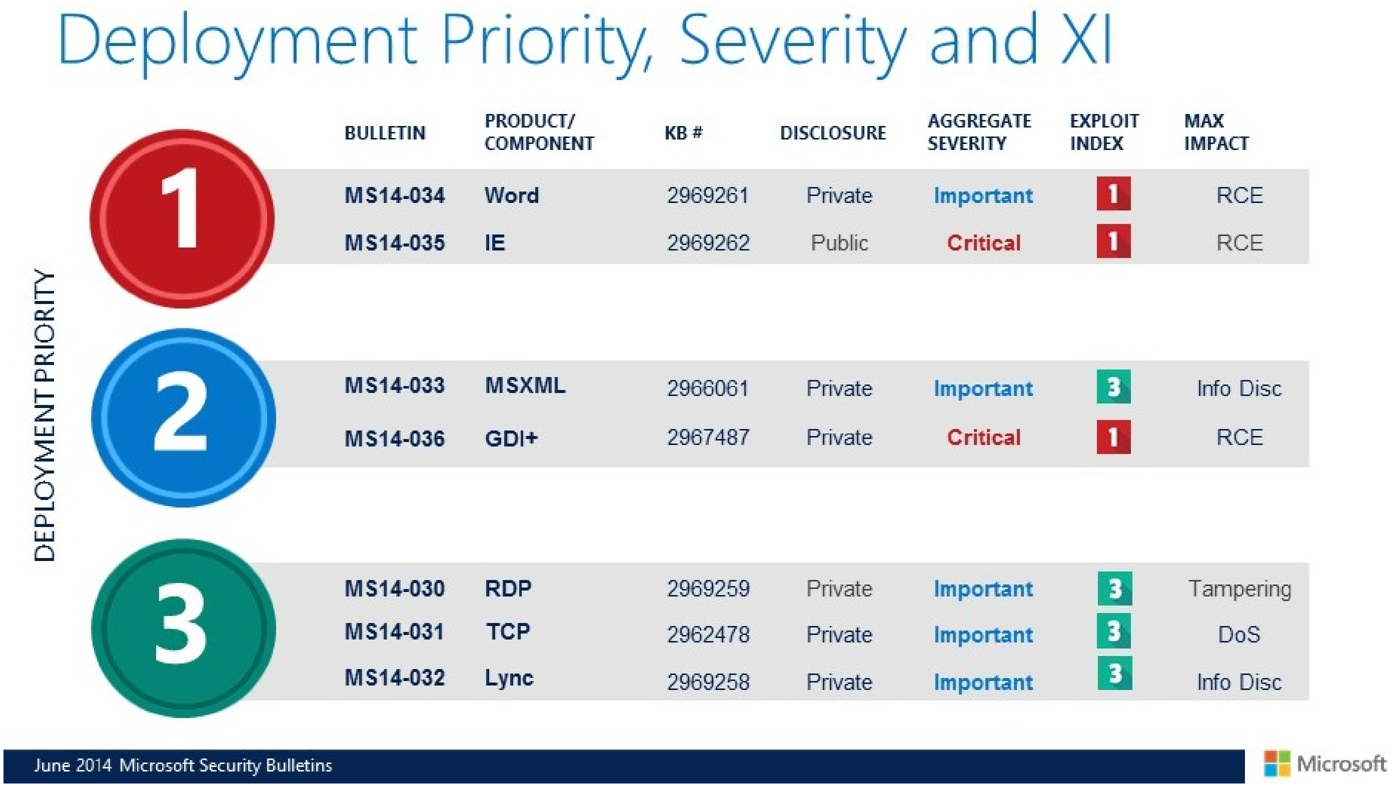
**Link Tracking Warning!**
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

## This week on Security Now!

- 2nd Tuesday with two Critical Vulnerabilities
- Google's browser-based PGP
- More OpenSSL troubles
- The first Internet IP Address Registry to hit critical IPv4 levels.
- iOS8 privacy news
- Nonsense from The Register (co.uk)
- News about network congestion, Netflix and Level3
- And interactions with our listeners

## Security News:

### Microsoft's 2nd Tuesday:



Deployment Priority, Severity and XI

| DEPLOYMENT PRIORITY | BULLETIN | PRODUCT/ COMPONENT | KB # | DISCLOSURE | AGGREGATE SEVERITY | EXPLOIT INDEX | MAX IMPACT |
|---|---|---|---|---|---|---|---|
| 1 | MS14-034 | Word | 2969261 | Private | Important | 1 | RCE |
| | MS14-035 | IE | 2969262 | Public | Critical | 1 | RCE |
| 2 | MS14-033 | MSXML | 2966061 | Private | Important | 3 | Info Disc |
| | MS14-036 | GDI+ | 2967487 | Private | Critical | 1 | RCE |
| 3 | MS14-030 | RDP | 2969259 | Private | Important | 3 | Tampering |
| | MS14-031 | TCP | 2962478 | Private | Important | 3 | DoS |
| | MS14-032 | Lync | 2969258 | Private | Important | 3 | Info Disc |

June 2014 Microsoft Security Bulletins

- Critical:
    - MS14-035: Internet Explorer Remote Code Execution
    - MS14-036: Windows Desktop & Server Remote Code Execution
        - Unicode Scripts Processor Vulnerability - CVE-2014-1817 (usp10.dll)
            - Appears to require "WebDAV" (Web Distributed Authoring and Versioning) and the WebClient service.
            - Requires remote access to ports 139 and 445 : Windows networking.
                - These are blocked by ISPs, Routers, and Windows firewall.

    - GDI+ Image Parsing Vulnerability - CVE-2014-1818
        - Disable Metafile processing

- Important:
    - MS14-034: Word 2007 SP3 & Office Compatibility -- Remote Code Execution
    - MS14-033: OS Information Disclosure

**Google's "End-To-End" encryption**

- https://code.google.com/p/end-to-end/
- I've given it a good look... and I'm impressed.
- Is "Secure JavaScript Crypto" an oxymoron?
- Timing attacks. / Memory attacks, etc.

**More bad news for OpenSSL:**

- https://www.sans.org/webcasts/98445
- https://www.openssl.org/news/secadv_20140605.txt
- https://www.imperialviolet.org/2014/06/05/earlyccs.html
- Possible MITM key material downgrade attack (null keys):
    - Requires vulnerable OpenSSL on each end.
    - Has been in the OpenSSL codebase for at least 15 years.
- DTLS CLient-side crash with an invalid handshake.
- Others requiring obscure non-default settings or API calls.

**More good news for iOS / v8 randomizes WiFi MAC addresses to thwart tracking.**

- Nice new feature, but overblown hype headlines:
- http://qz.com/218437/a-tiny-technical-change-in-ios-8-could-stop-marketers-spying-on-you/
- "A tiny technical change in iOS 8 could stop marketers spying on you."
- A great deal of non-connected WiFi tracking is going on.  iOS8 prevents that.

**The Register: Redmond is patching Windows 8 but NOT Windows 7, say security bods.**

- New tool checks differences, could lead to 0-day bonanza
- <quote> Microsoft has left Windows 7 exposed by only applying patches to its newest operating systems.

Researchers found the gaps after they scanned 900 Windows libraries and uncovered a variety of security functions that were updated in Windows 8 but not in 7. They said the shortcoming could lead to the discovery of zero day vulnerabilities.

The missing safe functions were part of Microsoft's dedicated libraries intsafe.h and strsafe.h that help developers combat various attacks.

Researcher Moti Joseph - formerly of Websense - speculated Microsoft had not applied fixes to Win 7 to save money.

"Why is it that Microsoft inserted a safe function into Windows 8 [but not] Windows 7? The answer is money - Microsoft does not want to waste development time on older operating systems ... and they want people to move to higher operating systems," Joseph said in a presentation at the Troopers14 conference.

**LACNIC / Latin America and the Caribbean:**

- http://www.lacnic.net/en/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac
- Headline: No more IPv4 addresses in Latin America and the Caribbean
- Subhead: Latin America and the Caribbean have entered the IPv4 exhaustion phase; the delay in deploying Internet Protocol version 6 in our region is cause for concern.
- <quote> 10 June.- Today, the Internet Address Registry for Latin America and the Caribbean (LACNIC), the organization responsible for assigning Internet resources in the region, announced the exhaustion of its IPv4 address pool and expressed its concern regarding the fact that operators and governments throughout the region are delaying the deployment of Internet Protocol version 6 (IPv6).

  LACNIC reported that its pool of available IPv4 addresses reached the 4,194,302 mark, and that this has triggered stricter Internet resource assignment policies for the continent. In practice, this means that IPv4 addresses are now exhausted for Latin American and Caribbean operators.

  LACNIC's CEO said: "This is an historic event; the fact that it was anticipated and announced doesn't make it any less significant. From now on, LACNIC and its National Registries will only be able to assign very small numbers of IPv4 addresses, and these will not be enough to satisfy our region's needs."

  Since it began operating in 2002, the organization has assigned more than 182 million IPv4 addresses throughout Latin America and the Caribbean.

  As agreed by the regional community, now that only 4,194,302 available IPv4 addresses (/10) remain, LACNIC's pool of IPv4 addresses is considered officially exhausted and the Gradual Exhaustion and New Entrants policies have come into effect, introducing new procedures and requirements for those requesting resources.

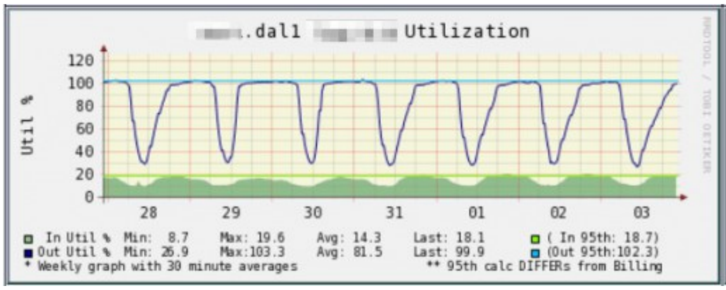
**Netflix now delivering poor connection notices. ISPs not happy**

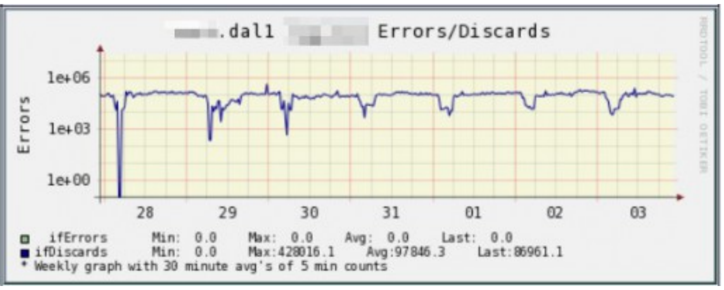
- http://blog.streamingmedia.com/2014/06/netflixs-network-congestion-message-rolling-networks-just-verizon.html
- Netflix said their goal in doing this is to help their subscribers understand when their experience is degrading based on their network provider (as opposed to their home WiFi, etc). When Netflix feels that many clients are experiencing congestion on a certain segment of a certain ISP's network, they will display the message for clients who are experiencing degradation.

**Level3:**

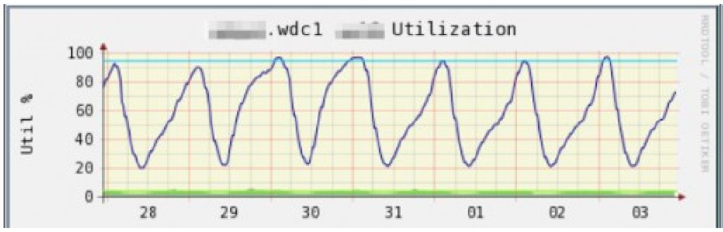
- http://blog.level3.com/global-connectivity/observations-internet-middleman/
- http://blog.level3.com/global-connectivity/chicken-game-played-child-isps-internet/

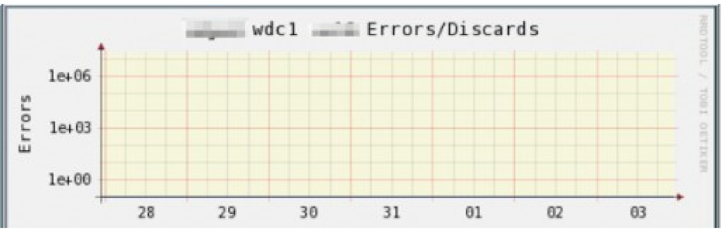
As an example, this is what one of those congested interconnections looks like. It is a 100Gbps interconnect in Dallas for the week ending April 3. The graph on the left shows flat tops for most of each day – the port is congested and cannot accept all of the traffic that is trying to get through. Not only are packets being dropped (the number dropped are on the right), but all those not being dropped are also subject to delay:





For comparison, below is an uncongested interconnection. This is also 100Gbps but in Washington, D.C. with another peer. This shows no congestion, although there isn't much headroom, so a capacity augment is underway. The graph on the right shows absolutely no dropped packets:





## Miscellany:

- **SMG's observed Chrome bloat was due to add-ons!**

- **Edge of Tomorrow**

- **Halt & Catch Fire:**
  - After 2nd episode, annoyed but watching...

- **Amazon uses TrueCrypt:**
  - http://aws.amazon.com/importexport/faqs/#Security
  - AWS only ships devices out of AWS facilities if the device is completely erased or the device only contains data encrypted by AWS. For import jobs, we erase devices after job completion. For export jobs, we will always encrypt the data being exported onto the device. We use TrueCrypt software for encryption.

## SQRL Update:

- S4 - SQRL Secure Storage System
- OCB vs GCM

## SpinRite:

From: "Erik Ellsinger" <info@erikellsinger.se>
Subject: Spinrite saved me from going crazy
Date: Fri, 06 Jun 2014 14:30:37 -0000
Location: Sweden

Hi

For a while now my computer has freezed up from time to time. It completely stopped responding to input, and the hard drive light was on constantly. It usually lasted for 10-30 seconds and then all was fine again. But lately it started to do that at least once every 5 min, which was driving me crazy because I got interrupted all the time with whatever I was doing.

I looked in the Win 8 task manager and saw that during the times the computer freezes the operating system hard drive is at 100% use. But the response time is 0ms and it's not reading or writing. But the hard drive has to be doing something, since the hard drive light on the computer is fully on. Has the hard drive encountered a sector it can't read and it's just retrying it until it gives up?

I've had SpinRite for a while now and thought I would give it a try. But I needed my computer for work so I waited to run it until school was over. After SpinRite was finished I booted Windows. And now, after using my computer for a day now I can say that the freezing problem is completely gone and cured and SpinRite saved me from going crazy!
Erik