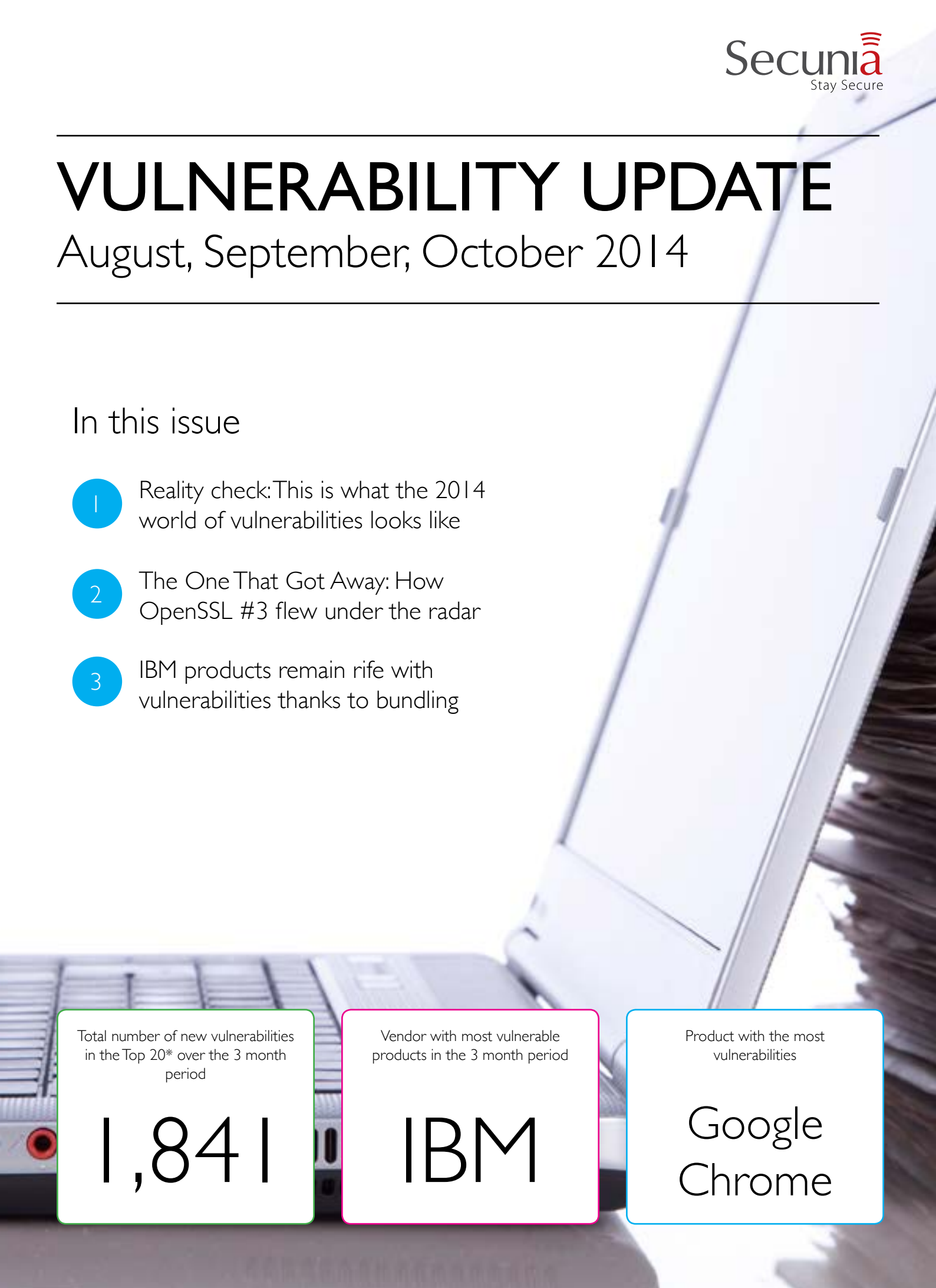
Secunia
Stay Secure

VULNERABILITY UPDATE

August, September, October 2014

In this issue



Total number of new vulnerabilities in the Top 20* over the 3 month period

1,841

Vendor with most vulnerable products in the 3 month period

IBM

Product with the most vulnerabilities

Google Chrome

1

Reality check: This is what the 2014 world of vulnerabilities looks like

While high-profile vulnerabilities in popular mainstream products like Windows, Flash and Java get most of the attention, it's worth pointing out that the Top 20 lists you find in this report represent the everyday vulnerability landscape.

Vulnerabilities are discovered and disclosed every day in products from a mix of vendors, and as the year is coming to an end we can safely say that the total number of vulnerabilities has increased – by around 40% from 2013 to 2014.

The 1,841 vulnerabilities listed here in the Top 20s span all the different criticalities and attack vectors, and while many of them had patches available on the day of disclosure, a lot of them did not. The applications they were discovered in cover a wide range of products used in a variety of business contexts; whether the individual vulnerability represents a specific threat to your organization, of course, depends solely on where and how you use the application.

You can find more information about the individual vulnerable products by logging in to the Secunia Community, search for the product using the Secunia Advisory ID (*) and read the detailed advisories:

www.secunia.com/community

2

The One That Got Away: How OpenSSL #3 flew under the radar

August saw 9 vulnerabilities in Open SSL. In itself not dramatic, but interesting nonetheless, because this is what we refer to as "OpenSSL Take 3" and it represents the quintessence of what the IT industry should learn from The Big Three of 2014: Heartbleed/OpenSSL, Shellshock/Bashbug and POODLE. Essentially, what we saw was that if you give a vulnerability a catchy name and get it some publicity, all the vendors of the world scrambled to uncover if the vulnerability is in their products, and hurry to create and publish a patch for it. No publicity means no disclosure and no patches.

It went like this: When news broke about OpenSSL Take 1 (a.k.a Heartbleed) more than 100 vendors had issued patches for 600 products made vulnerable by Heartbleed within just 40 days. The same thing happened 2 months later, when OpenSSL Take 2 revitalized the hype from the first round. Within the first 40 days we saw around 600 affected products, but in the following weeks, an additional 200 products were pronounced vulnerable through OpenSSL, bringing the grand total to 800 products.

However, when Take 3 happened, the media had lost interest – and with the hype gone, less than 20 vendors took the time to disclose and patch some 50 products. 100 days in, the number of affected products is at 75. Consequently, not only are there products that are vulnerable and unpatched because of "OpenSSL Take 3", but they are also undisclosed. And that is really bad!

3

IBM products remain rife with vulnerabilities thanks to bundling

IBM products are vulnerable – in 2013 Secunia reported 4,000 vulnerabilities in IBM products, which meant that IBM vulnerabilities accounted for 25% of the total number of vulnerabilities reported in 2013.
In 2014, nothing has changed: several IBM products are on the Top 20 lists for August, September and October, and their position is largely due to the fact that IBM likes to bundle the products with third-party software – very often with vulnerable libraries like Java and OpenSSL.

That these programs are bundled within the individual IBM product means that every single time a vulnerability is discovered and a patch released for e.g. Java, the corresponding IBM products needs to be updated, too. First by IBM, and then by all IBM customers.

Anyone running IBM products knows that in the weeks and months following an Oracle Patch Day, they need to get busy patching their IBM applications. All in all, a very time consuming process.

TOP 20

Secunia
Stay Secure

AUGUST 2014

SECUNIA ID	VULNS	PRODUCT
24179	64	Google Chrome
31330	58	Oracle Solaris
34544	41	EMC RSA Archer GRC
34586	37	IBM Tivoli Application Dependency Discovery Manager
35791	29	IBM Notes (formerly IBM Lotus Notes)
37195	29	IBM Domino (formerly IBM Lotus Domino)
8706	28	IBM Lotus Notes
11842	28	IBM Lotus Domino
31722	26	IBM Tivoli Endpoint Manager
12493	24	Microsoft Internet Explorer
30393	24	Juniper Network and Security Manager
55502	24	WordPress Mobiloud Plugin
11764	20	HP Service Manager
55373	20	F5 ARX Series
37026	16	Juniper Security Threat Response Manager
10134	15	IBM Java
33836	15	IBM WebSphere Real Time
36360	15	WHMCS
2683	14	Cacti
15878	9	OpenSSL

OCTOBER 2014

SECUNIA ID	VULNS	PRODUCT
24179	162	Google Chrome
1352	159	Avant Browser
916	83	Apple iTunes
34908	34	IBM Security Network Intrusion Prevention System
18571	32	Sun Solaris
2372	30	Apple Macintosh OS X
11826	30	IBM CICS Transaction Gateway
15593	29	Oracle Database
31330	29	Oracle Solaris
35794	28	IBM Tivoli Storage Productivity Center
30352	25	Oracle Java JRE
30476	25	Oracle Java JDK
4762	22	Cisco IOS XE
10177	22	IBM WebSphere Message Broker
37776	22	IBM Integration Bus
55963	20	IBM FlashSystem
5215	19	Cosminexus Application Server
5919	19	Cosminexus Developer
5920	19	Cosminexus Studio
12666	19	Mozilla Firefox

SEPTEMBER 2014

SECUNIA ID	VULNS	PRODUCT
2372	59	Apple Macintosh OS X
22334	43	VMware vCenter Server
12493	38	Microsoft Internet Explorer
31731	37	VMware vSphere Update Manager
1674	24	Adobe Flash Player
31330	21	Oracle Solaris
2367	20	Apple iOS for iPad
2368	20	Apple iOS for iPod touch
2864	20	Apple iOS for iPhone and later
34938	20	IBM InfoSphere Guardium
56097	20	IBM TS3000 (TSSC)
57224	20	IBM InfoSphere Guardium Database Activity Monitor
12666	19	Mozilla Firefox
32427	18	IBM Storwize Unified
24179	17	Google Chrome
31086	17	F5 TMOS
36351	17	F5 BIG-IP Access Policy Manager
14874	16	Net-SNMP
33501	16	Apple OS X Server
2215	15	AIX

*: Definition of the Top 20: The Top 20 are the 20 products with the most vulnerabilities in the specified month, out of the more than 50,000 products verified by Secunia Research, and recorded in the Secunia Vulnerability Database. The Secunia ID identifies the product. Secunia Advisories cover vulnerabilities announced for all types of programs and operating systems.