Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE
ANALYSIS

June 2015

Commonly exploited software vulnerabilities targeting critical networks

Introduction

1. This product provides an overview of the most common application vulnerabilities that were exploited to target critical infrastructure organisations and networks of national importance.

2. This assessment was developed in collaboration with our partners in the United States, United Kingdom, Canada, and New Zealand. The prioritised vulnerabilities and corresponding mitigation measures outlined in this document represent the shared judgement of all participating entities.

Software Vulnerabilities and Patching

3. The threat vectors frequently used by cyber adversaries such as malicious email attachments, links in emails to compromised websites, “watering holes” and other techniques often take advantage of unpatched vulnerabilities found in widely used applications.

4. The longer an application remains unpatched, the longer it is vulnerable to compromise. Once a patch has been publicly released, the patch can be reverse-engineered by cyber adversaries to create an exploit. This process has been observed to take as little as 24 hours.

5. It is important that organisations establish a robust patch management process to ensure that timely and comprehensive patching of applications occurs. Patching applications is one of the most effective steps an organisation can take to minimise its exposure to threats facing its network.

Most Commonly Exploited Vulnerabilities

6. The ACSC, in collaboration with partners in the United States, United Kingdom, Canada and New Zealand, has identified the following vulnerabilities as frequently exploited by cyber adversaries.

7. Publicly known vulnerabilities are tracked with the Common Vulnerabilities and Exposures (CVE) system (https://cve.mitre.org/). This system creates a unique identifier for all new vulnerabilities, establishing a standard reference for information security professionals.

Microsoft Office

CVE	Affected Products / Versions	Patching Information
CVE-2008-2244	Word 2002 SP3 and Word 2003 SP2/SP3	Mitigation information
CVE-2009-3129	Office 2008 for Mac, Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2, Office Excel 2002 SP3, Office Excel 2003 SP3, Office Excel 2007 SP1 and SP2, Office Excel Viewer 2003 SP3, Office Excel Viewer SP1 and SP2, Open XML File Format Converter for Mac	Mitigation information
CVE-2010-3333	Office 2003 SP3, Office 2004 for Mac, Office 2007 SP2, Office 2008 for Mac, Office 2010, Office for Mac 2011, Office XP SP3, Open XML File Format Converter for Mac	Mitigation information
CVE-2011-0101	Excel 2002 SP3	Mitigation information
CVE-2012-0158	BizTalk Server 2002 SP1, Commerce Server 2002 SP4, Commerce Server 2007 SP2, Commerce Server 2009 Gold and R2, Office 2003 SP3, Office 2003 Web Components SP3, Office 2007 SP2 and SP3, Office 2010 Gold and SP1, SQL Server 2000 SP4, SQL Server 2005 SP4, SQL Server 2008 SP2/SP3/ R2, Visual Basic 6.0 Runtime, Visual FoxPro 8.0 SP1, Visual FoxPro 9.0 SP2.	Mitigation information
CVE-2012-1856	Commerce Server 2007 SP2,Commerce Server 2009 Gold and R2, Host Integration Server 2004 SP1, Office 2003 SP3, Office 2003 Web Componenent SP3, Office 2007 SP2 and SP3, Office 2010 SP1, SQL Server 2005 SP4, SQL Server 2008 SP2/SP3/ R2/ R2 SP1/R2 SP2, Visual Basic 6.0 Runtime, Visual FoxPro 8.0 SP1.	Mitigation information
CVE-2014-1761	Office Compatibility Pack PS3, Office for Mac 2011, Office Web Apps 2010 SP1 and SP2, Office Web Apps Server 2013, Office Word 2003 PS3, Office Word 2007 SP3, Office Word 2010 SP1/SP2, Office Word 2013/2013 RT, Office Word Viewer, Sharepoint Server 2010 SP1/ SP2, Sharepoint Server 2013.	Mitigation information
CVE-2014-4114	Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2008 SP2/R2 SP1, Windows Server 2012 Gold/ 8.1, and Windows Vista SP2.	Mitigation information

Microsoft Internet Explorer

CVE	Affected Products / Versions	Patching Information
CVE-2006-3227	Internet Explorer 6	Mitigation information
CVE-2009-3674	Internet Explorer 8	Mitigation information
CVE-2010-0806	Internet Explorer 6, 6 SP1 and 7	Mitigation information
CVE-2012-4792	Internet Explorer versions 6, 7 and 8	Mitigation information
CVE-2013-1347	Internet Explorer 8	Mitigation information
CVE-2014-0322	Internet Explorer 9 and 10	Mitigation information
CVE-2014-1776	Internet Explorer 6, 7, 8, 9, 10 and 11	Mitigation information

Microsoft Silverlight

CVE	Affected Products / Versions	Patching Information
CVE-2013-0074	Silverlight 5 and 5 Developer Runtime	Mitigation information

Oracle Java

CVE	Affected Products / Versions	Patching Information
CVE-2012-1723	Java Development Kit and JRE 7 Update 21 and earlier Java Development Kit and JRE 6 Update 32 and earlier Java Development Kit and JRE 5 Update 35 and earlier	Oracle Java information on CVE-2012-1723
CVE-2013-2465	Java Development Kit and JRE 7 Update 21 and earlier Java Development Kit and JRE 6 Update 32 and earlier Java Development Kit and JRE 5 Update 35 and earlier	Oracle Java information on CVE-2012-2465

Adobe ColdFusion

CVE	Affected Products / Versions	Patching Information
CVE-2013-0625	Versions 9.0 to 9.02 and 10	ColdFusion Security hotfix APSB13-03
CVE-2013-0632	Versions 9.0 to 9.02 and 10	ColdFusion Security hotfix APSB13-03
CVE-2013-3336	Versions 9.0 to 9.02 and 10	ColdFusion Security hotfix APSB13-13
CVE-2013-5326	Versions 9.0 to 9.02 and 10	ColdFusion Security hotfix APSB13-27

Adobe Reader

CVE	Affected Products / Versions	Install latest version of:
CVE-2010-2883	Adobe Reader - Versions 9.x and earlier	• Adobe Reader for Windows • Adobe Reader for Macintosh • Adobe Reader for UNIX
CVE-2011-2462	Adobe Reader - Versions 9.x and earlier	• Adobe Reader for Windows • Adobe Reader for Macintosh • Adobe Reader for UNIX
CVE-2013-2729	Adobe Reader – Versions 9.x and earlier; Versions 11.x before 11.0.03 are affected	• Adobe Reader for Windows • Adobe Reader for Macintosh • Adobe Reader for UNIX

Adobe – Multiple Platforms

CVE	Affected Products / Versions	Patching Information
CVE-2009-3953	Adobe Acrobat - Versions 9.4.4 and earlier Adobe Reader - Versions 9.x and earlier	• Acrobat Standard and Pro 10.x and 9.x users on Windows can find the appropriate update here. • Acrobat Pro Extended 9.x users on Windows can find the appropriate update here. • Acrobat Pro users on Macintosh can find the appropriate update here. • Acrobat 3D for Windows can find the appropriate update here.
CVE-2010-0188	Adobe Acrobat - Versions 9.4.4 and earlier Adobe Reader - Versions 9.x and earlier	
CVE-2011-0611	Adobe Acrobat - Versions 10.0.3 and earlier	**Adobe Acrobat**: Versions 10.0.3 and earlier should be updated by following the below links. • Acrobat Standard and Pro 10.x and 9.x users on Windows can find the appropriate update here.

	Adobe Air - Versions 15.0.0.0293 and earlier Adobe Flash Player - Versions 10.2.154.27 and earlier, 13.x to 13.0.0.244 and 15.0.0.167 and earlier Adobe Reader - Versions 10.1.1 and earlier	- Acrobat Pro Extended 9.x users on Win dows can find the appropriate update here. - Acrobat Pro users on Macintosh can find the appropriate update here. - Acrobat 3D for Windows can find the appropriate update here. **Adobe Air**: Versions 15.0.0.0293 and earlier should be updated to the latest version of Adobe AIR. **Adobe Flash Player**: Upgrade to the latest version of Adobe Flash Player **Adobe Reader**: Versions 10.1.1 and earlier should be updated by following the below links. - Adobe Reader for Windows - Adobe Reader for Macintosh - Adobe Reader for UNIX
CVE-2014-0564	Adobe Air - Versions 15.0.0.0293 and earlier Adobe Flash Player - Versions 10.2.154.27 and earlier, 13.x to 13.0.0.244 and 15.0.0.167 and earlier Adobe SDK & Compiler - Versions prior to 15.0.0.302	**Adobe** Air: Versions 15.0.0.0293 and earlier should be updated to the latest version of Adobe AIR **Adobe Flash Player:** Adobe recommends users of the Adobe Flash Player Extended Support Release should update to version 13.0.0.250 by visiting here. **Adobe SDK & Compiler:** Versions prior to 15.0.0.302 should be updated to the latest version of Adobe AIR SDK & Compiler

OpenSSL

CVE	Affected Products / Versions	Patching Information
CVE-2014-0160	OpenSSL v 1.0.0 - 1.0.1f Known as the Heartbleed vulnerability, this vulnerability affects OpenSSL v 1.0.0 - 1.0.1f that could expose private data to a remote, unauthenticated attacker through an incorrect memory handling function in the TLS heartbeat extension. This could allow a remote attacker to decrypt secure traffic and expose credentials and secret keys. OpenSSL is a popular application commonly used in web browsing, emails and instant messaging to provide security and privacy. Note OpenSSL is commonly used on Apache software running on Linux/Unix platforms, but is also employed by a number of other Linux/Unix services. Further details of vulnerable services can be found through the National Vulnerability Database.	It is recommended that system administrators test and deploy the vendor released updates to affected platforms accordingly. For clients unable to immediately upgrade, consider disabling OpenSSL Heartbeat support. For more information: National Vulnerability Database

Mitigation Strategies

8. As part of a comprehensive security strategy, the ACSC recommends that organisations implement the top four strategies from ASD's *Strategies to Mitigate Targeted Cyber Intrusions*. These are :

   i. use application whitelisting to help prevent malicious software from executing

   ii. patch application vulnerabilities

   iii. patch operating system vulnerabilities

   iv. restrict administrative privileges to systems and applications based on user duties.

9. The combination of all four strategies, correctly implemented in a mature state, will help protect an organisation from low to moderately sophisticated intrusion attempts.

10. The ACSC recommends that partners review the full list of *Strategies to Mitigate Targeted Cyber Intrusions*. These strategies are designed to be flexible to meet the needs of different organisations, allowing every organisation to assess the risk to its information and systems and act accordingly.

Contact details

11. Australian government customers with questions regarding this advice should contact the ACSC on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

12. Australian businesses or other private sector organisations seeking further information should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.

Further information

13. Assessing Security Vulnerabilities and Patches
http://www.asd.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Patches.pdf