

Fructuoso Rivera 387 - 6 'A'
X5000BOG - Córdoba
Argentina

T. 054-351-4866554
C. 054-9-341-5030941
feliam@binamuse.com

Felipe Andrés Manzano

I worked in security almost uninterruptedly since 2005. First as pentester and then diving into the deepest of application security, reverse engineering and exploitation.

The last few years I study some aspects of dynamic program analysis and wrote a python tool for the symbolic execution of amd64 Linux binaries. <https://github.com/feliam/pysymemu>

I've released 10+ CVEs and exploits, got a nomination in 2010 pwnie awards, researched in depth the PDF file format <http://feliam.wordpress.com/2010/08/23/opaf/>, and gave a couple of talks in small hacker and academic conferences.

Technical skills

Software Development	C, Python, C++, Java
Assemblers	Intel, sparc
Operating Systems	Linux, OSX, Windows, Solaris

Education

01/2010–	PHD Candidate in <i>Computer Science</i> at FAMaF, University of Cordoba, Argentina.
01/1997–09/2005	Bachelor Degree in <i>Computer Science</i> at FCEIA, University of Rosario, Argentina. (5 years diploma)
01/1992–11/1996	High School at Politécnico Superior Gral. San Martín institute, University of Rosario, Argentina. Qualifications obtained in Electronics.

Work Experience

2008–	Security Researcher at Binamuse
02/2007–03/2008	Exploit Writer at CORE Security Technologies
09/2005–02/2007	Junior security consultant at Flowgate

Publications / cool CVEs / Honors

2014-09-21	CVE-2014-4377, Apple CoreGraphics Memory Corruption
2014-09-21	CVE-2014-4378, Apple CoreGraphics Information Disclosure
2013-09-27	PySymEmu: A symbolic execution engine for AMD64. Ekoparty
2013-07-18	CVE-2013-3665, Autodesk Multiple Products DWG Processing Array Indexing Vulnerability
2013-05-23	CVE-2013-366[234], SketchUp Memory Corruption and Buffer Overflow Vulnerabilities
2013-05-15	CVE-2013-27[29—30], Adobe Reader / Acrobat Multiple Vulnerabilities
2012-05-09	CVE-2012-2026, Adobe Illustrator Multiple Vulnerabilities
2010-09-29	CVE-2010-3429, FFmpeg Multiple Vulnerabilities
2010-09-14	CVE-2010-3624, Adobe Reader/Acrobat Multiple Vulnerabilities
2010-04-14	CVE-2010-0201, Adobe Reader/Acrobat Multiple Vulnerabilities

Publications / cool CVEs / Honnors (continued)

2009-12-15 CVE-2009-2994, Adobe Reader/Acrobat Multiple Vulnerabilities
2009-10-28 Right Hemisphere Products U3D Parsing Array Indexing Vulnerability
2009-10-09 CVE-2009-2994, Adobe Reader/Acrobat Multiple Vulnerabilities
2009-03-01 Speaker at uCon, Recife, Brazil. *Hacking PDF readers*
2009-09-30 CVE-2008-3827, MPlayer "demux_real_fill.buffer()" Buffer Overflow Vulnerabilities
2008-07-08 CVE-2008-2950, Poppler "pageWidgets" Uninitialized Memory Access
2008-02-26 CVE-2008-0984. VLC media player chunk context validation error.
2008-02-04 CVE-2008-0485. Quicktime file MPlayer arbitrary pointer dereference.
2005-08-31 M. Cristiá, F. Manzano, G. Giusti *The implementation of Lisex, a MLS Linux Prototype*
ASSE 2005, 34ta JAIIO, Rosario, Argentina.

References upon request.