



UNIVERSITÀ TELEMATICA eCAMPUS
Ufficio Ricerca e Sviluppo



UNIVERSITÀ DEGLI STUDI DI
GENOVA



FONDAZIONE
BRUNO KESSLER



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Novedrate, 26 marzo 2012
Comunicato stampa

TEAM DI RICERCA ITALIANO RIPARA UN BACO DI ANDROID

La vulnerabilità avrebbe potuto essere facilmente sfruttata da applicazioni software malevole, con l'effetto di rendere completamente inutilizzabili i dispositivi attualmente in commercio basati sul sistema operativo di Google. La soluzione *made in Italy* si è rivelata efficace e verrà inserita in un prossimo aggiornamento.

Un gruppo di ricercatori italiani ha individuato e neutralizzato una seria vulnerabilità presente in tutte le versioni di Android, il diffuso sistema operativo sviluppato da Google appositamente per gli smartphones ed i tablet PC.

L'importante risultato è il frutto di una collaborazione tra ricercatori che operano in diversi atenei e centri di ricerca italiani: il prof. **Alessio Merlo** (Università Telematica E-Campus, Dipartimento di Ingegneria), il prof. **Alessandro Armando**, responsabile dell'Unità di Ricerca "Security & Trust" della Fondazione Bruno Kessler di Trento e coordinatore del Laboratorio di Intelligenza Artificiale del DIST all'Università di Genova, il prof. **Mauro Migliardi** (coordinatore del gruppo Green, Energy Aware Security dell'Università di Padova) e **Luca Verderame** (neo-laureato in Ingegneria Informatica dell'Università di Genova).

Il team di ricercatori ha segnalato prontamente la vulnerabilità a Google e al Security Team di Android, fornendo una dettagliata analisi dei rischi relativi. Ha quindi progettato una soluzione che è stata verificata dal Security Team di Android e che - vista l'efficacia - sarà adottata in uno dei prossimi aggiornamenti del sistema operativo.

Se non fosse stata neutralizzata, la vulnerabilità scoperta dal team italiano avrebbe permesso ad un'applicazione software malevola (malware) di saturare le risorse fisiche del dispositivo, portando al blocco completo sia degli smartphones che dei tablet PC con il sistema operativo Android. Un problema particolarmente insidioso poiché l'applicazione malevola in questione non richiederebbe alcuna autorizzazione in fase di installazione e tenderebbe quindi ad apparire innocua all'utente.

L' importante risultato del team di ricerca italiano verrà pubblicato negli atti del congresso internazionale 27th IFIP International Information Security and Privacy Conference - SEC 2012 (Heraklion, Crete, Greece, June 4-6, 2012). Una parte di questo lavoro è stato co-finanziato nell'ambito del progetto europeo FP7-257876 SPaCIoS (<http://www.spacios.eu/>).

Informazioni tecniche

La vulnerabilità individuata si basa su un difetto nel controllo della comunicazione tra applicazioni e componenti vitali di Android che permette di esaurire sistematicamente le risorse di memoria del dispositivo mediante la generazione di un numero arbitrariamente grande di processi. Il principio fondamentale della sicurezza di Android è la totale separazione tra le applicazioni (sandboxing) per garantire che ognuna di queste non possa inficiare in alcun modo il funzionamento delle altre. Il team dei ricercatori italiani ha dimostrato come questa separazione sia violata nei sistemi correnti e ha indicato la soluzione per poterla nuovamente garantire.

Risorse:

A. Armando, A. Merlo*, M. Migliardi, L. Verderame, "Would you mind forking this process? A Denial of Service attack on Android (and some countermeasures)" disponibile in versione pre-print su: <http://www.ai-lab.it/merlo/publications/DoSAndroid.pdf>.

Contatti:

Prof. Alessio Merlo

Dipartimento di Ingegneria,
Università E-campus.
Tel.: 3289199105
Email: alessio.merlo@uniecampus.it
Web: <http://www.ai-lab.it/merlo>

Prof. Alessandro Armando

Security & Trust
Center for Information Technology
Fondazione Bruno Kessler, Trento
Email: armando@fbk.eu
Tel.: 3281003201
Web: <http://st.fbk.eu>
Dipartimento di Informatica, Sistemistica e Telematica (DIST)
Università degli Studi di Genova
Email: armando@dist.unige.it
Web: <http://www.ai-lab.it/armando/>

Prof. Mauro Migliardi

Dipartimento di Ingegneria dell'Informazione

Università di Padova

Tel.: 3281003221

email: mauro.migliardi@unipd.it

Web: <http://harness.cipi.unige.it/migliardi/index.html>

Ing. Luca Verderame

Dipartimento di Informatica, Sistemistica e Telematica (DIST)

Università degli Studi di Genova

Tel.: 3494920084

email: luca.verderame@ai-lab.it