Nota vulnerabilità processori Intel, AMD e ARM

Gestione	Azienda	Riferimento
REDATTO:	Telecom Italia S.p.A.	
REDATTO:	Enterprise Services Italia S.r.l. - A DXC Technology Company	
APPROVATO:	Telecom Italia S.p.A. (Mandataria), Enterprise Services Italia S.r.l. - A DXC Technology Company	
N° allegati:	0	

In data 3 Gennaio 2018 è stata resa nota dai Vendor la vulnerabilità dei processori Intel immessi sul mercato a partire dal 1995 (eccetto i modelli Itanium e Atom precedenti al 2013) e la parziale vulnerabilità dei processori AMD e ARM, incluse le versioni *mobile*.
Ref. (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/ https://www.ibm.com/blogs/psirt/potential-cpu-security-issue/)

Si tratta di due vulnerabilità di tipo *side channel* denominate Meltdown (CVE-2017-5754) e Spectre (CVE-2017-5753 e CVE-2017-5715) che hanno impatto su diverse architetture CPU e che consentono l'accesso non autorizzato alle aree di memoria del Sistema Operativo.

Tali vulnerabilità sono state riscontrate nelle funzionalità di *speculative execution* implementate dalla maggior parte delle CPU per massimizzare la performance tramite l'esecuzione anticipata di parti di codice. Esse non consentono ad un attaccante di accedere da remoto ad un sistema, ma potrebbero consentire a chi ha già accesso ad un sistema, apparato o dispositivo vulnerabile, di accedere a dati sensibili. E' stato infatti dimostrato dai ricercatori dei Vendor come le suddette vulnerabilità rendono possibile l'accesso ad aree di memoria del Sistema Operativo, normalmente non accedibili senza i corretti privilegi, che potrebbero potenzialmente contenere dati come chiavi crittografiche, password, ecc.
Ref. (https://googleprojectzero.blogspot.dk/2018/01/reading-privileged-memory-with-side.html).

I nostri team di specialisti si sono immediatamente adoperati per collaborare con le ingegnerie dei vendor HW al fine di garantire sui sistemi operativi gestiti dal RTI il massimo livello di sicurezza possibile.

Al momento Intel (processore alla base delle architetture su cui sono implementate le piattaforme SPC Cloud) ha rilasciato una prima versione del microcode aggiornato ed a seguire i vendor HW hanno rilasciato un primo firmware update, che è stato ritirato dopo qualche giorno perchè provocava dei riavvi spontanei dei sistemi, sono tutt'ora in corso gli sviluppi per una fix stabile.

Al fine di mitigare le possibili minacce derivanti da tali vulnerabilità, in attesa del rilascio di patch risolutive, sottolineiamo l'importanza di password di accesso robuste e sistemi antivirus funzionanti ed aggiornati.
Il team sta lavorando per rilasciare la funzionalità di autenticazione a due fattori che incrementa ulteriormente il livello di sicurezza della piattaforma e contribuisce quindi alla mitigazione del rischio.