Skrivet av Erik Liljencrantz
2014-09-25 10:37 - Senast uppdaterad 2014-09-25 11:20

Den 24:e september 2014 publicerade RedHat info om Bash-buggen och kallade den "katastrofal, värre än heartbleed". Vi har uppdaterat våra system och skall därför inte drabbas.
Programmet bash används i Linux-servrar, i Apple-datorer och en del Android-enheter för att tolka kommandon och finns därför i alla dessa system. Nu upptäcktes att vissa argument till kommandon hanterades på ett sätt som gav en hacker möjlighet att få fulla rättigheter på maskinen. Till vår Linux CentOS var man snabbt ute med en patch så vi kunde köra "yum update bash" som svarade: Resolving Dependencies --> Running transaction check ---> Package bash.x86_64 0:4.1.2-15.el6_4 will be updated ---> Package bash.x86_64 0:4.1.2-15.el6_5.1 will be an update --> Finished Dependency Resolution och strax därefter skall inte bash-buggen kunna missbrukas på våra system.

Vill man testa om ett system är sårbart kan följande (ofarliga) kommando köras i bash: env x='() { :;}; echo vulnerable' bash -c "echo this is a test" så blir utmatningen på ett sårbart system: vulnerable this is a test Efter åtgärd visas istället: bash: varning: x: ignoring function definition attempt bash: fel vid import av funktionsdefinition för "x" this is a test där extra data efter funktionsdefinitionen ger ett felmeddelande istället för att köras med potentiellt förhöjd behörighet.

Med denna artikel vill vi dels visa vikten av att uppdatera sina system, vilket vi gör, men också erbjuda vår kompetens när det gäller drift och underhåll av Linux-servrar och nätverk.

Redhats artikel om bash-buggen:
https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/
Lättare artikel i PC för Alla:
http://www.idg.se/2.1085/1.584888/ny-sarbarhet-drabbar-bade-linux-och-mac