Urgentní bezpečnostní opatření pro terén

ref. č. **Identifikátor:**	**GPS_2012_07.1** IVD produkty: problém se Symantec pcAnywhere **GC-0493119**
Typ akce:	**Nápravné opatření pro terén**
Datum vystavení dokumentu:	**4. července 2012**

Detailní popis ovlivněného prostředku a/nebo systému:

Název produktu	**Číslo součásti**	**Číslo šarže**	**Expirace**
Datová stanice AMPLILINK (všechny verze)	03516440001	N/A	N/A
IVD přístroj MagNA Pure 96	06541089001	N/A	N/A
LightCycler 1.2 (CE-IVD, US-IVD)*	12011468301	N/A	N/A
LightCycler 2.0 (CE-IVD, US-IVD)*	03531414001	N/A	N/A
cobas® 8000 data manager (všechny verze)	05511976001	N/A	N/A
COBAS INTEGRA® 400	28065047001	N/A	N/A
COBAS INTEGRA® 400 plus	03245233001	N/A	N/A

*pouze ve spojení se schválenými IVD testy od Roche

Shrnutí problému	Chyba v Symantec pcAnywhere. Chyba v "Symantec pcAnywhere" (verze 12.6.6 a starší) umožňuje počítačovým pirátům přečíst, změnit nebo vymazat tak důležité informace jakými jsou výsledky testů, elektronicky chráněné zdravotnické informace a auditovanou stopu na dotčených ovládacích PC systémů Roche.
Souhrn požadovaných opatření	Roche Diagnostics nabízí pro dotčené ovládací PC několikero způsobů nápravy, prosím podívejte se do sekce *"Opatření, která může udělat uživatel"*
Kontakty	Technický servis: Hotline tel: 220 382 505 Product Manager: Mgr. David Čermák, tel: 602 487 381 Product Manager: Ing. Petr Kopecký, tel: 602 511 901 Země: Česká republika

Popis problému:

Symantec informoval na zasedání bezpečnostní rady Roche o chybě ve svém produktu pcAnywhere (verze 12.6.6 a starší), v softwarovém produktu pro vzdálený přístup do PC. Touto chybou je takzvaná "před-ověřovací zranitelnost", která umožňuje plný přístup k cílovému systému bez nutnosti se přihlásit. Tato zranitelnost umožňuje počítačovým pirátům číst, měnit a mazat takové důležité údaje, jakými jsou výsledky testů, údaje o pacientech a auditovaná stopa.
Zároveň může být ovlivněna i šifrovaná informace, pokud je šifrovací klíč uložen na stejném systému.

Vyhodnocení rizika:

SHRNUTÍ:
Ačkoliv současná pravděpodobnost výskytu při různých pirátských scénářích je „velmi nízká“ až „teoretická“, pokud by se měl tento problém vyskytnout, mohla by být ovlivněna integrita a správnost pacientských výsledků. To by vedlo k vážným zdravotním důsledkům. Odhalení škodlivého softwaru není pravděpodobné.

Opatření, která může udělat uživatel:

Všechna nápravná opatření budou provedena buď přes vzdálený přístup nebo přímo zástupcem Roche Diagnostics.
U produktů uvedených v **tabulce 1** se po zákazníkovi nevyžadují **žádná opatření**.

Tabulka 1: Seznam produktů nevyžadujících od zákazníka žádné opatření

Název produktu
Data Station AMPLILINK (všechny verze)
cobas® 8000 data manager (všechny verze)
COBAS INTEGRA® 400
COBAS INTEGRA® 400 plus

U produktů uvedených v **tabulce 2**, **pouze** pokud se používají ve spojení s **IVD testy Roche**, prosím kontaktujte Vašeho lokálního reprezentanta Roche Diagnostics, který provede další kroky.

Tabulka 2: Seznam produktů, které vyžadují zásah uživatele

Název produktu
IVD přístroj MagNA Pure 96
LightCycler 1.2 LC (CE-IVD, US-IVD)*
LightCycler 2.0 (CE-IVD, US-IVD)*

* pouze ve spojení se schválenými IVD testy od Roche

K dnešnímu dni není znám **žádný případ** útoku na pcAnywhere v systémech Roche Diagnostics a útok je čistě teoretický. Roche Diagnostics nicméně dokončí kroky vedoucí k nápravě situace v průběhu příštích 6 měsíců.

Omlouváme se za nepříjemnosti, které Vám v souvislosti s tímto problémem mohly nastat.

S pozdravem

Mgr. David Čermák
PM IT Solution

Radoslav Blažek
BA Manager ProfDia