Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

Sérülékenység kezelés
Tanácsok szoftvergyártóknak

2012. szeptember

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalomjegyzék

Bevezetés

A gyártók szempontjából a szoftvereikben található sérülékenységekről szóló információk közlése és nyilvánosságra kerülése akár a szoftverek nem megfelelő minőségének mérőszáma is, amely hatással lehet egy adott cég szoftver eladásaira is. Éppen ezért a ”bizonytalanságon alapuló biztonság” elve széles körben elterjedt, azaz semmilyen, vagy csak minimális információk kerülnek nyilvánosságra még legsúlyosabb sérülékenységekről is. Ez a gondolkodásmód vezethet az olyan esetekhez, amikor a támadók már részletes információval rendelkeznek az ilyen sérülékenységekről, akár a saját kutatásaik alapján, akár úgy, hogy biztonsági szakemberektől veszik a leírásokat. A támadók aztán kihasználhatják ezeket a sérülékenységeket és az ebből eredő károkat az adott szoftver használói szenvedik el. Mindezek mellett, a harmadik felek nem mindig követik az összehangolt közzététel (avagy felelősségteljes közzététel) elveit, amikor információt hoznak nyilvánosságra egy általuk felfedezett sérülékenységről. Az összehangoltság ez esetben azt jelenti, hogy a sérülékenységet bizalmasan jelentik a gyártó felé és vele közösen dolgozzák ki a megfelelő, a hibát javító frissítést és a sérülékenységről szóló információt csak ezután teszik közzé. Az ok, amiért a szakemberek gyakran nem követik a felelősségteljes közzététel elveit az, hogy a gyártók gyakran biztosítanak erre megfelelő kommunikációs csatornát, vagy egyszerűen nem reagálnak a kezdeti megkeresésekre.

Ezen dokumentum a szoftverek és egyéb IT termékek (beleértve a firmware gyártókat is) gyártói számára tartalmaz tanácsokat a sérülékenységek megfelelő kezeléséről. Ebbe bele értendő a céges belső előkészítés, a megfelelő kommunikációs csatornák felállítása, a konkrét incidenskezelés és az utómunkálatok is. Azok a gyártók, akik követik ezeket a tanácsokat kiemelkedhetnek a konkurens cégek közül és akár profitálhatnak is a ügyfelek elégedettségéből.

Belső előkészítés

A gyártóknak még azelőtt fel kell készülniük az incidensek kezelésére, mielőtt egy adott termék sérülékenységét felfedeznék. A sérülékenységek kezelését mindenek előtt a cégen belül kell irányítani. Ez a következőket foglalja magában:

- Közzétételi szabályozás
- Szerepek és jogosultságok (Ki mit csinál / hoz döntést?)
- Belső folyamatok, beleértve a határidőket (válaszidő), amely kiterjed a sérülékenység megértésére és reprodukálására, a megoldás kidolgozására és javítócsomagok elkészítésére és tesztelésére
- Annak tudatosítása, hogy a termékek sérülékenységeinek professzionális kezelésére, mind a vásárlóknak, mind pedig a sérülékenységek bejelentői számára szükségesek

A közzétételi szabályozás, vagy sérülékenység kezelési eljárás egy olyan iránymutató, amely leírja, hogy az adott gyártó miként foglalkozik a sérülékenységekkel. Ez a szabályozás igen fontos, mivel ez segít kiépíteni a bizalmat a gyártók és a sérülékenységek keresésével foglalkozó biztonsági kutatók között. Ennek elsődleges célja, hogy részletes információt adjon arról, hogy a gyártó miként értelmezi, illetve alkalmazza az összehangolt közzététel elveit és ez mit jelent a biztonsági kutatók számára. Ennek tartalmaznia kell egy állásfoglalást arról a gyakorlatról, hogy a gyártó a bizalmasság jegyében miként kezeli a kutatók adatait, az esetleges nyilvánosságra hozásról, és azt, hogy mit várnak el a kutatóktól. Emellett fontos, hogy részletesen információt biztosítson, arról hogy a sérülékenység javítására milyen folyamatokat alkalmaz a cég és milyen módon érinti ez a kutatókat. Előfordulhat például, hogy a gyártó megtiltja a szakembereknek, hogy az általuk felfedezett

sérülékenységet a médiában vagy biztonsági konferencián bármilyen formában publikálják.

Annak érdekében, hogy a gyártók ne ijesszék el a kutatókat, nem kötelezhetik őket olyan jogi megállapodások vagy szerződések aláírására, mint az együttműködési megállapodás[1] vagy a titoktartási nyilatkozat[2] és fontos, hogy a kutatók biztosítva legyenek arról, hogy a gyártó nem perli be őket, legalábbis amíg ők betartják a gyártó által lefektetett alapszabályokat. A nyilvánosságra hozatali szabályozásnak továbbá tartalmazni kell, hogy a kutatók mire számíthatnak a gyártótól ideértve a különböző esetleges sérülékenység felfedezési díjazásokat.

Kommunikációs csatornák

A megfelelő kommunikációs csatornák a gyártók, a vásárlók és a biztonsági kutatók között alapvető fontosságú a hatékony és rövid távú sérülékenység kezelésben. Nem ajánlott egyetlen dedikált ember a biztonsági ügyek kezelésére, mivel egy ilyen alkalmazott kiesése komoly problémákat okozhat. Ehelyett kapcsolattartási pontot érdemes felállítani, majd ezt elérhetővé tenni a vállalat weboldalán, valamint a termékek dokumentációjában.

A gyártók számára a weboldalaikon központi helyen érdemes a biztonsághoz köthető információkat közzétenni, amely igaz az általános (pl. https://www.gyártó.com/biztonság) és a konkrét programokhoz köthető információkra (pl. https://www.gyártó.com/terméknév/biztonság) is. Az ilyen oldalakon az SSL használata kötelező.

A biztonsághoz köthető oldalaknak tartalmaznia kell:

- sérülékenységi információt (riasztások a még nem javított sérülékenységekkel kapcsolatban, információk a workarond-okkal és közleményekkel (bulletin) kapcsolatban, továbbá, hogy mely frissítések érhetőek el).
- A termékek biztonságához tartozó kapcsolati információt (e-mail cím, telefonszám ügyeleti idő megjelölésével, publikus PGP kulcsok és S/MIME tanúsítványok a bizalmas kommunikáció biztosítására)
- a vállalat közzétételi szabályozását
- frissítéseket és hibajavításokat
- a programok biztonságos használatához kapcsolódó kiegészítő dokumentumokat (tanulmányok, GY.I.K)
- kommunikációs űrlapot, amely lehetővé teszi a gyártónak, hogy rendszerezze az információ folyamot és hogy bizonyos információ megadását kötelezővé tegye. Emellett az ilyen űrlapok lehetőséget biztosítanak a névtelen sérülékenységi bejelentésre is.

Ezeket az oldalakat érvényes és igazolható SSL tanúsítványokkal kell védeni, hogy biztosítva legyen az közzétett információ hitelessége és bizalmassága. A biztonsággal kapcsolatos kérdésekhez tartozó központi e-mail címnek érdemes egyértelmű címet választani, mint például product-security@gyártó.com, security-team@gyártó.com, productname.security@cégnév.com vagy secure@cégnév.com. A security@cégnév.com cím használata nem javasolt, mivel az RFC 2142-es szabvány szerint ez a cím más célt szolgál.

1 MoU - Memorandum of Understanding
2 NDA - Non-Disclosure Agreement

A biztonsággal kapcsolatos kérdéseket, vagy a gyártó által biztosított kommunikációs csatornákon beérkező bejelentéseket 24 órán belül meg kell válaszolni egy személyes levél formájában, nem pedig egy automatikusan generált válaszüzenetben. A részletes elemzés után, ha lehetséges, 48-72 órán belül érdemes bővebb információval szolgálni a bejelentőnek.

A gyártók mindezek mellett levelezőlistát is fenntarthatnak a biztonsággal kapcsolatos kérdések számára. Ezeket a leveleket a gyártó oldalához használt digitális aláírással és tanúsítvánnyal kell védeni. Ilyen weboldalak például:

- http://osvdb.org/vendors
- http://oss-security.openwall.org/wiki/vendors
- http://ocert.org/team_and_members.html

Kapcsolat a harmadik felekkel

Javasolt egy olyan hálózat felállítása, amelyben a harmadik félnek számító szervezetek részt tudnak venni, hogy rövid időn belül tudjanak reagálni az eseményekre, különösen akkor, ha a sérülékenységnek rendkívüli hatása van. Ide tartoznak a kormányzati szervezetek, mint például a német BSI, ipari szervezetek, más országbeli CERT-ek. Különösen az olyan termékek esetén van szükség erre, amelyeknek nagy hatása van a kritikus infrastruktúrára (Németország KRITIS, Egyesült Államok CIKR), ahol a BSI-hez hasonló intézmények segíthetnek a fontos információk terjesztésében. Rendkívül hasznos, ha részletes információk állnak rendelkezésre az országokról, iparágakról és forgatókönyvekről, amelyekben az adott termékek használatban vannak. Továbbá a CERT-hez történő regisztráció segíthet a gyártóknak abban, hogy értesüljenek a legújabb figyelmeztetésekről és tanácsokról, amelyek az ő saját termékeiket és infrastruktúrájukat érinthetik. Az is hasznos lépés, ha kapcsolatot tartanak a versenytársakkal, partnerekkel és más szervezetekkel, mint például az iparági szakmai fórumok és tesztlaborok.

A főbb gyártókat illetve az elterjedt protokollokat és technológiákat érintő sérülékenységek miatt különösen fontos, hogy az iparágon belül legyen információ csere. Különösen a harmadik féltől származó kód, mint egy keretrendszer vagy programkönyvtár tekintetében kell körültekintően eljárni, amikor a biztonságról van szó, mivel az ilyen harmadik féltől származó kód felhasználásával az már az adott gyártó termékének része lesz. Ezért egy biztonsági kapcsolatot kell létrehozni minden ilyen felhasznált komponens gyártójához, és az azok által kiadott figyelmeztetéseket legalább napi szinten ellenőrizni ajánlott, és a kiadott riasztásokban, hírlevelekben, figyelmeztetésekben leírtakat a megfelelő módon alkalmazni. Ezek lehetnek a javítócsomagok backport-olása, komponensek frissítése, riasztások kiadása.

Előállhatnak olyan helyzetek, amikor kiderül, hogy a biztonsági rés fő oka a harmadik féltől származó komponens sérülékenysége. Erről a leggyorsabban értesíteni kell a termék gyártóját. Minden érintett félnek konstruktívan kell eljárnia, hogy meg lehessen oldani az összetett problémát, illetve ugyanazt a konstruktivitást és erőfeszítést kell tanúsítani, ha egy másik gyártó érintett egy olyan sérülékenység miatt, ami a saját termékben van.

Az incidensek kezelése

A külső kommunikáció legfontosabb eszköze a sérülékenységek kezelésében a riasztások és bulletin-ek. Egy riasztásnak a következőket kell tartalmaznia:

- a riasztás címe vagy azonosítója (pl. szisztematikus és következetes számozás)
- a publikáció dátuma
- az érintett termékek, verziók és konfigurációk
- az érintett platformok és operációs rendszerek
- kritikusság (alacsony, közepes, magas besorolás) és a becsült kockázati besorolás a CVSS[3] alapján
- következmények (pl. szolgáltatás megtagadás, távoli kód végrehajtás, helyi jogosultság kiterjesztés, stb.)
- a sérülékenység rövid leírása
- részletes leírás (a technikai személyzetnek)
- a hibajavítás vagy frissítés várható ideje
- a sérülékenységhez köthető események időrendi felsorolása
- lehetséges megoldások
- a sérülékenység felfedezésének értékelése
- a sérülékenység bejelentésének vagy nyilvánosságra hozatalának módja (pl. összehangolt közzététel)
- információ arról, hogy az sérülékenységhez tartozó exploit vagy proof-of-concept (PoC) kód nyilvánosságara került-e
- a riasztás szerzője
- CVE szám vagy CVE Candidate referencia szám[4]
- kiegészítő információ
- URL a riasztás legfrissebb verziójához

Ha a riasztás frissítették, akkor a módosított vagy hozzáadott részeket egyértelműen kell jelölni. A riasztásnak nem szabad olyan információt tartalmaznia, amely alapján egy képzett szakember kihasználhatja a szóban forgó sérülékenységet. Tilos emellett a sérülékenységet bemutató vagy az érintett rendszerek ellenőrzését szolgáló exploit vagy proof-of-concept (PoC) kód közlése, mivel azt azonnal kihasználhatják. A riasztást a gyártó weboldalán is található titkosítási kulcsokkal kell aláírni és a riasztásnak tartalmazni kell egy linket a titkosítási kulcsokhoz. Amint elérhetővé válik a frissítés vagy hibajavítás az érintett sérülékenységhez, a riasztást közleménnyé (bulletin) kell alakítani, amelynek további információt tartalmaz a frissítésről. Ide tartozik az, hogy honnan lehet a frissítést letölteni, milyen lehetséges kompatibilitási problémák adódhatnak és, hogy mi a teendő ha a frissítés valamiért egy adott rendszeren nem alkalmazható. A riasztásokat és a közleményeket (bulletin) nyilvánosságra kell hozni amint lehetséges, de a publikáció minőségét és pontosságát nem szabad, hogy a határidők befolyásolják.

3 Common Vulnerability Scoring System. http://first.org/cvss
4 http://cve.mitre.org

Következmény

A sérülékenységkezelést követően érdemes összegezni a incidens kezelés közben szerzett tapasztalatokat, hogy a sérülékenység kezelés melyik részén érdemes még javítani. Az ilyen estekből további tanulságot lehet levonni a fejlesztési folyamatok javítása és a minőségirányítás tekintetében. Ez további minőség ellenőrzési pontok vagy tesztelési módszerek megjelenését eredményezheti.