SILENT SIGNAL
VÉSZJELZÉS HELYETT...

1. Bevezető

A dokumentum összefoglalja a Silent Signal Kft. szakértőinek 2011-ben elért kutatási és fejlesztési eredményeit. Ebben az időszakban munkatársaink 16 sebezhetőséget azonosítottak elterjedt üzleti szoftverekben és hozzájárultak három szabad szoftveres biztonsági projekt fejlesztéséhez is. Hisszük, hogy munkánkkal sikerült részt vennünk a világ IT rendszereinek biztonságosabbá tételében, és reméljük, hogy ezt a munkát legalább ilyen eredményesen tudjuk folytatni 2012-ben is.

2. Sérülékenységek

Az alábbi hibák jelentős része zero day kategóriába tartozik, ezért a szakértők csak minimális információkat publikálhatnak az egyes sérülékenységekkel kapcsolatosan. A hibák felfedezése után biztonsági közvetítő cégeken keresztül a gyártók értesítése megtörtént. Jelen hibalistának nem célja a károkozásra vagy egyéb törvénybe ütköző cselekedetre buzdítás.

Gyártó: Symantec
Sérülékenység típusa: Távoli fájlhozzáférés
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
Az adminisztrátori felületen autentikáció nélkül elérhető egy hibakezelő almodul, melynek segítségével az appliance-en található fájlokhoz lehetséges hozzáférni a webszerver jogaival. A hibát egy nem ellenőrzött, felhasználó által befolyásolható változó okozza.

Gyártó: Symantec
Sérülékenység típusa: Távoli fájlhozzáférés, parancsvégrehajtás
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
A kiadási megjegyzések megjelenítésért felelős almodul segítségével a fájlrendszeren tárolt fájlokhoz lehetséges hozzáférni, valamint megfelelő paraméterekkel operációs rendszer parancsokat is végre lehet hajtani. A hibát egy nem ellenőrzött, felhasználó által befolyásolható változó okozza.

Gyártó: Symantec
Sérülékenység típusa: Távoli fájlhozzáférés, törlés, fájl feltöltés
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
A kártékonynak ítélt fájlok letöltését végző funkció segítségével bármilyen fájl letölthető a rendszerből, amely a folyamat végén root jogosultsággal törlésre is kerül. A hiba segítségével két, egyébként htaccess-szel védett fájl feltöltési funkciót is engedélyezni lehet, így operációs rendszer szintű parancsvégrahajtást lehet megvalósítani.

Gyártó: Symantec
Sérülékenység típusa: Parancsvégrehajtás
Autentikáció szükséges: igen
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
Egy nem támogatott (ám ennek ellenére el nem távolított) konfiguráció-ellenőrző modulban speciális escape szekvenciák segítségével operációs rendszer szintű parancsokat lehet végrehajtani.

Gyártó: National Instruments
Sérülékenység típusa: Távoli parancsvégrehajtás
Autentikáció szükséges: nem
Felhasználói interakció szükséges: igen
Kockázati besorolás: közepes

Hiba leírása:
Egy hibás ActiveX modulon keresztül puffer-túlcsordulást lehetséges előidézni, amely segítségével akár operációs rendszer parancsokat is végre lehet hajtani a futtatást végző felhasználó jogaival.

Gyártó: IBM
Sérülékenység típusa: Távoli fájlhozzáférés
Autentikáció szükséges: igen
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
A naplófájlok megjelenítését végző almodul segítségével a rendszeren tárolt fájlokhoz lehetséges hozzáférni.

Gyártó: IBM
Sérülékenység típusa: Távoli parancsvégrehajtás
Autentikáció szükséges: nem
Felhasználói interakció szükséges: igen
Kockázati besorolás: közepes

Hiba leírása:
Egy hibás ActiveX modulon keresztül puffer-túlcsordulást lehetséges előidézni, amely segítségével akár operációs rendszer parancsokat is végre lehet hajtani a futtatást végző felhasználó jogaival.

Gyártó: Schneider Electric
Sérülékenység típusa: Távoli parancsvégrehajtás
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
SCADA szoftver SSL implementációjában található hiba segítségével operációs rendszer szintű parancsokat lehet végrehajtani.

Gyártó: Schneider Electric
Sérülékenység típusa: Távoli parancsvégrehajtás
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
Egy manager service a kapott bemeneti adatokat egy statikus méretű pufferbe másolja. Megfelelően összeállított bemenet elküldésével operációs rendszer parancsokat is végre lehet hajtani.

Gyártó: National Instruments NI
Sérülékenység típusa: Távoli parancsvégrehajtás
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
A szolgáltatás a felhasználók kiszolgálása során olyan fájlokat is kezel, melyek a felhasználó befolyása alatt állhatnak. Megfelelően összeállított, formázó karaktereket tartalmazó fájlnéven és elérési úton keresztül a program működése befolyásolható.

Gyártó: Cisco
Sérülékenység típusa: Távoli parancsvégrehajtás
Autentikáció szükséges: igen
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
Hálózati menedzsment szoftver autentikáció után elérhető részében escape szekvenciák segítségével operációs rendszer parancsok hajthatók végre privilegizált jogkörrel.

Gyártó: Cisco
Sérülékenység típusa: Távoli fájlhozzáférés
Autentikáció szükséges: igen
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
Autentikáció után elérhető modul segítségével bármilyen, az operációs rendszerben található fájlt el lehet érni.

Gyártó: HP
Sérülékenység típusa: Adatbázis manipuláció
Autentikáció szükséges: nem
Felhasználói interakció szükséges: nem
Kockázati besorolás: magas

Hiba leírása:
A menedzsment szoftver webszolgáltatásának egy metódusa nem megfelelően ellenőrzi a felhasználóktól származó adatokat, ezért metakarakterek használatával az adatbázis közvetlenül manipulálható.

Gyártó: Aruba
Sérülékenység típusa: Perzisztens Cross-Site Scripting
Autentikáció szükséges: nem
Felhasználói interakció szükséges: igen
Kockázati besorolás: közepes

Hiba leírása:
A jelentésgeneráló komponens nem megfelelően szűri a környező Access Pointok adatait, ezért egy támadó egy speciális AP üzembe helyezésével parancsokat hajthat végre a bejelentkezett adminisztrátor nevében.

Gyártó:	Oracle
Sérülékenység típusa:	Jogosultság-kiterjesztés
Autentikáció szükséges:	nem
Felhasználói interakció szükséges:	nem
Kockázati besorolás:	közepes

Hiba leírása:
A naplófájlok megjelenítését végző almodul segítségével a rendszeren tárolt fájlokhoz lehetséges hozzáférni.

Gyártó:	Ericsson
Sérülékenység típusa:	Directory Traversal
Autentikáció szükséges:	nem
Felhasználói interakció szükséges:	nem
Kockázati besorolás:	magas

Hiba leírása:
Az Open Telecom Platform `inets:httpd` könyvtárának hibája lehetővé teszi a dokumentum gyökéren túli fájlok elérését Windows rendszeren futó alkalmazások esetében.

3. Szabad szoftveres hozzájárulások

A szabad szoftverek eszköztárunk nélkülözhetetlen részét képezik. A szabad felhasználásért cserébe mi is részt vállalunk ezen programok tesztelésében, karbantartásában és fejlesztésében.

Projekt:	Wireshark
URL:	`http://www.wireshark.org`
Hozzájárulás:	MySQL dissector modul

Projekt:	Browser Exploitation Framework
URL:	`https://github.com/beefproject/beef`
Hozzájárulás:	Tesztelés és hibajavítás

Projekt:	mitmproxy
URL:	`http://mitmproxy.org/`
Hozzájárulás:	Optimalizálás és kódminőség javítása