CARNET

Upute za tumačenje izvještaja provjere ranjivosti (Nessus® v.8.11)

CERT.hr-PUBDOC-2020-7-401

Sadržaj

1 UVOD

S ciljem unapređenja sigurnosti mreže i mrežom dostupnih servisa, CARNET poduzima različite akcije, između ostaloga i provjeru ranjivosti računalnih mreža članica CARNET-a. Cilj ovog dokumenta je upoznati Vas s postupkom provjere ranjivosti, alatom koji je korišten za provedbu istoga, te Vam olakšati tumačenje dobivenih rezultata provjere ranjivosti računalne mreže Vaše ustanove i poduzimanje potrebnih radnji s ciljem otklanjanja pronađenih sigurnosnih ranjivosti.

2 O RANJIVOSTIMA

Ranjivost (eng. *vulnerability*) je slabost računalnog sustava koju je moguće slučajno aktivirati ili namjerno iskoristiti, te na taj način nanijeti štetu tom sustavu. Ranjivost također možemo opisati i kao stanje ili skup stanja koja mogu omogućiti nekoj prijetnji da utječe na resurse ustanove. One se mogu pojaviti u bilo kojem dijelu računalnog sustava, a najčešće ih nalazimo u korisničkim programima i operativnom sustavu zbog grešaka u programskom kodu. Osim toga, ranjivosti se mogu pojaviti i zbog neprikladnog korištenja računalnih programa ili pogrešno podešene konfiguracije uređaja.

Bez obzira na uzrok, mjesto nastanka ili utjecaj na računalni sustav, iskorištavanjem određenih ranjivosti napadač može dobiti potpunu kontrolu nad sustavom, te ukrasti, izmijeniti ili obrisati podatke odnosno učiniti sustav djelomično ili potpuno nedostupnim. Na ranjiva računala napadači, između ostaloga, postavljaju zlonamjerne programe koji im omogućavaju daljnje napade na druge sustave. Zbog toga je važno voditi računa o redovitom ažuriranju operativnog sustava računala i pripadajućih programa te koristiti programe i uređaje prema sigurnosnim smjernicama za njihovu uporabu.

3 POSTUPAK PROVJERE RANJIVOSTI

Postupak provjere ranjivosti obuhvaća prikupljanje podataka o sigurnosnim problemima na računalima i drugim uređajima spojenima na Internet te uputama za njihovo uklanjanje. Za prikupljanje podataka najčešće se koriste specijalizirani alati za provjeru ranjivosti (eng. *vulnerability scanneri)*, računalni programi koji korištenjem različitih tehnika skeniraju uređaje u određenom IP rasponu mreže, te na temelju tako prikupljenih podataka dolaze do informacija o topologiji i strukturi mreže, vrsti i tipu uređaja, inačici operativnog sustava uređaja, popisu otvorenih portova i sl. Prikupljenim podacima specijalizirani alati za provjeru ranjivosti pridružuje informacije o pronađenim ranjivostima, odnosno informacije o poznatim ranjivostima vezanima za određenu vrstu i tip uređaja, inačicu operativnog sustava, određeni TCP/UDP port i sl. te generira odgovarajući izvještaj. U određenim situacijama, s obzirom na metodologiju obavljanja provjere ranjivosti i korištene postupke, za dio pronađenih ranjivosti može biti riječ o lažno pozitivnom rezultatu, tj. situaciji da je *scanner* na određenom sustavu pronašao ranjivost, a da na sustavu ona zapravo ne postoji.

U postupku provjere ranjivosti računalne mreže Vaše ustanove korišten je Nessus® vulnerability scanner.

Nessus® je jedan od najpoznatijih alata za provjere ranjivosti (*eng. scanner)* koji putem skeniranja portova (*eng. portscan)* odnosno sondiranjem otvorenih portova računala iz pojedinog IP raspona, dolazi do informacija o pokrenutim servisima. U narednim koracima se, ovisno o konfiguraciji Nessusa® te podacima o vrsti i tipu pronađenih uređaja odnosno njihovih drugih značajki, provode dodatna testiranja kako bi se prikupili svi relevantni podaci o udaljenim uređajima odnosno utvrdilo postojanje određenih sigurnosnih ranjivosti. Nessus® trenutno podržava više od 140,000 modula *(eng. plugin)* za otkrivanje različitih vrsta ranjivosti. Sam modul obično sadrži informacije o ranjivosti, uputu korisniku kako potvrditi postojanje određene ranjivosti te upute za uklanjanje iste.

4 IZVJEŠTAJ PROVJERE RANJIVOSTI

Nakon provedenog postupka provjere ranjivosti generiraju se dva PDF izvještaja na engleskom jeziku koji sadrži opise sigurnosnih ranjivosti pronađenih skeniranjem računalne mreže Vaše ustanove, kao i upute za njihovo otklanjanje.

Ovisno o razini rizika razlikujemo sljedeće kategorije ranjivosti:

CRITICAL	sigurnosne ranjivosti kritičnog rizika
HIGH	sigurnosne ranjivosti visokog rizika
MEDIUM	sigurnosne ranjivosti srednjeg rizika
LOW	sigurnosne ranjivosti niskog rizika
INFO	informacije o otkrivenim servisima i obavljenim provjerama

Kritične sigurnosne ranjivosti predstavljaju najveću opasnost za Vaš sustav i uglavnom se odnose na programske pakete i operacijske sustave za koje više ne postoji podrška proizvođača odnosno za zastarjele inačice kojima je potrebna hitna nadogradnja. Ako postoje poznate ranjivosti za takve programske pakete i operacijske sustave, iste predstavljaju trajnu prijetnju za Vaš sustav. Iz tog razloga potrebno je u što kraćem roku ažurirati zastarjele operativne sustave i programske pakete. Uzmimo na primjer da koristite zastarjeli operativni sustav koji sadrži poznate ranjivosti koje potencijalnom napadaču omogućuju preuzimanje i potpunu kontrolu nad sustavom. Dobivanjem kontrole nad ranjivim poslužiteljem napadač je u mogućnosti pristupiti povjerljivim informacijama te ih izmijeniti, kopirati ili obrisati, iskoristiti poslužitelj kako bi, u Vaše ime, izveo napad na druge sustave ili u potpunosti onemogućio funkcioniranje ranjivog poslužitelja. Bez mogućnosti nadogradnje Vaš sustav je trajno izložen napadima, te ugrožava sigurnost cijelog sustava.

Sigurnosne ranjivosti visokog rizika predstavljaju gotovo jednaku prijetnju kao i kritične sigurnosne ranjivosti, te su kao takve posebno velika opasnost za Vaš sustav. Iz tog razloga potrebno ih je što prije ukloniti prema uputama koje se nalaze u izvještaju. Uzmimo na primjer da se u Vašoj mreži nalazi poslužitelj s ranjivom inačicom operativnog sustava ili programskog paketa za koji je poznato da sadrži ranjivost prelijevanja memorijskog među-spremnika (eng. *buffer overflow*). Napadač može iskoristiti ovu ranjivost kako bi izvršio proizvoljan kod na ranjivom poslužitelju

te na taj način zadobio potpunu kontrolu nad njim. Dobivanjem kontrole nad ranjivim poslužiteljem napadač je u mogućnosti pristupiti povjerljivim informacijama te ih izmijeniti, kopirati ili obrisati, iskoristiti poslužitelj kako bi, u Vaše ime, izveo napad na druge sustave ili u potpunosti onemogućio funkcioniranje ranjivog poslužitelja.

Sigurnosne ranjivosti srednjeg rizika predstavljaju ranjivosti nešto niže razine sigurnosnog rizika, ali su također prilično velika prijetnja ako se ne provedu odgovarajuće mjere zaštite. Uzmimo za primjer da Vaš poslužitelj prihvaća i ostvaruje vezu koristeći SSL 2.0 enkripciju koja je zastarjela i za koju su poznati višestruki sigurnosni propusti. Napadač može iskoristiti spomenute propuste kako bi se ubacio u komunikaciju između korisnika i poslužitelja (eng. *Man-In-The-Middle attack*). Na taj način sve poruke koje se izmjenjuju između korisnika i poslužitelja prvo vidi napadač, što mu daje mogućnost čitanja ili promjene sadržaja poruke. Na taj način napadač može saznati i osjetljive podatke kao što su korisnička imena i lozinke, što se kasnije može iskoristiti za daljnje napade na Vaš sustav, ili kako bi koristio određene mrežne servise u Vaše ime, odnosno koristeći ukradene korisničke podatke.

Sigurnosne ranjivosti niskog rizika predstavljaju propuste koji uključuju otkrivene servise koji se mogu iskoristiti za otkrivanje sporednih informacija o računalima i uređajima u mreži. Iako ove ranjivosti pripadaju kategoriji ranjivosti s najnižom razinom rizika, preporučujemo i njihovo otklanjanje. Potencijalni napadač može iskoristiti ovako prikupljene informacije za daljnje planiranje napada na određeni sustav.

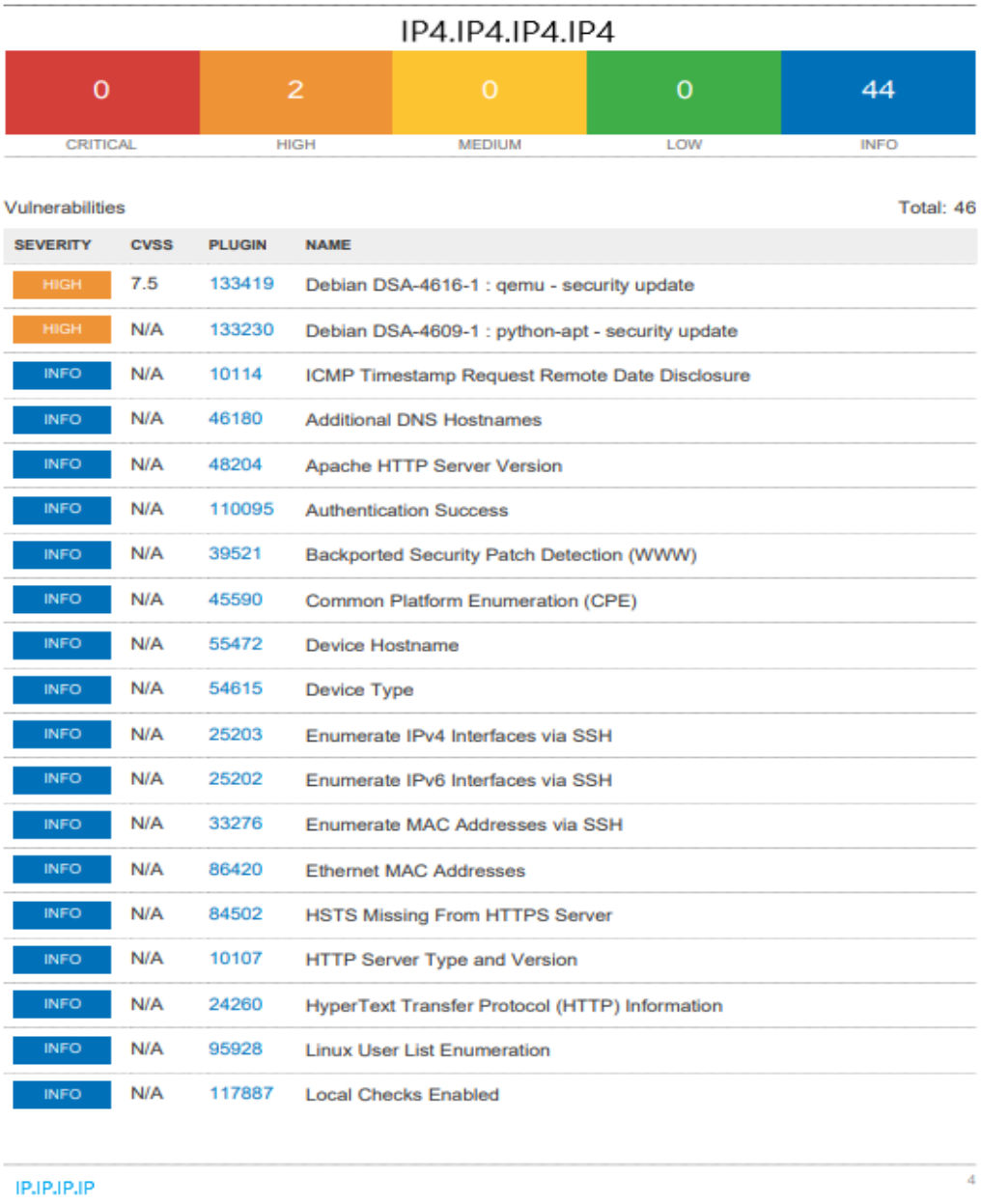
Posljednja kategorija zapravo ne predstavlja ranjivosti nego informacije o otkrivenim servisima, otvorenim portovima te informacije o obavljenim provjerama kao što su trajanje provjere, inačica alata koji je korišten, inačica skupine modula koji su korišteni i slično. Izvještaj provjere ranjivosti sadrži dva dokumenta koja se sastoje od nekoliko cjelina čiji sadržaj kratko komentiramo u nastavku.

Posljednja kategorija zapravo ne predstavlja ranjivosti nego informacije o otkrivenim servisima, otvorenim portovima te informacije o obavljenim provjerama kao što su trajanje provjere, inačica alata koji je korišten, inačica skupine modula koji su korišteni i slično.

Izvještaj provjere ranjivosti sadrži dva dokumenta koja se sastoje od nekoliko cjelina čiji sadržaj kratko komentiramo u nastavku.

4.1 Sažeti izvještaj provjere ranjivosti

Ovaj PDF dokument daje brzi pregled sigurnosnog stanja Vašeg sustava. Za svaki uređaj prikazan je sažetak obavljene provjere ranjivosti brojem ranjivosti koje su zastupljene u pojedinoj kategoriji, te ukupnim brojem otkrivenih ranjivosti, kao što je prikazano na Slika 1.



IP4.IP4.IP4.IP4

0	2	0	0	44
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 46

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	133419	Debian DSA-4616-1 : qemu - security update
HIGH	N/A	133230	Debian DSA-4609-1 : python-apt - security update
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	110095	Authentication Success
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	55472	Device Hostname
INFO	N/A	54615	Device Type
INFO	N/A	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	33276	Enumerate MAC Addresses via SSH
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	95928	Linux User List Enumeration
INFO	N/A	117887	Local Checks Enabled

IP.IP.IP.IP 4

Slika 1: Primjer sažetog izvještaj provjere ranjivosti

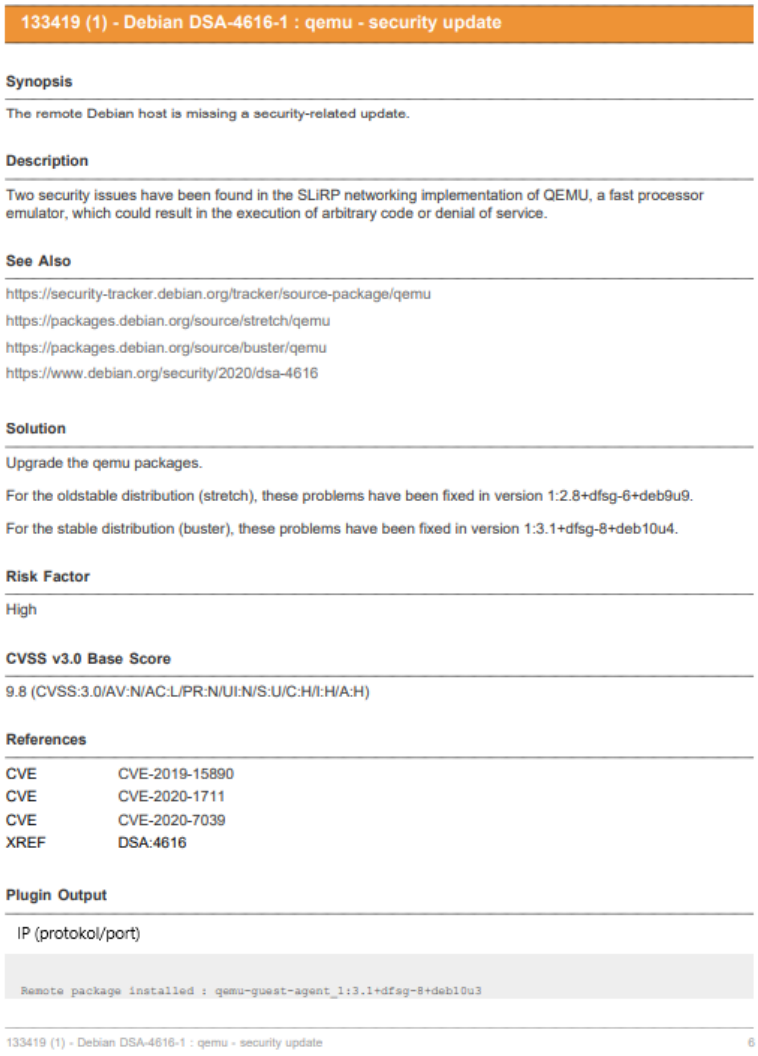
4.2 Detaljan izvještaj provjere ranjivosti

Detaljan izvještaj provjere ranjivosti sadrži popis svih ranjivosti koji su Nessus® moduli otkrili te detaljan ispis istih:

TABLE OF CONTENTS

Vulnerabilities by Plugin

Slika 2:Tablica sadržaja detaljnog izvješća



133419 (1) - Debian DSA-4616-1 : qemu - security update

Synopsis

The remote Debian host is missing a security-related update.

Description

Two security issues have been found in the SLiRP networking implementation of QEMU, a fast processor emulator, which could result in the execution of arbitrary code or denial of service.

See Also

https://security-tracker.debian.org/tracker/source-package/qemu
https://packages.debian.org/source/stretch/qemu
https://packages.debian.org/source/buster/qemu
https://www.debian.org/security/2020/dsa-4616

Solution

Upgrade the qemu packages.

For the oldstable distribution (stretch), these problems have been fixed in version 1:2.8+dfsg-6+deb9u9.

For the stable distribution (buster), these problems have been fixed in version 1:3.1+dfsg-8+deb10u4.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

References

CVE	CVE-2019-15890
CVE	CVE-2020-1711
CVE	CVE-2020-7039
XREF	DSA:4616

Plugin Output

IP (protokol/port)

```
Remote package installed : qemu-guest-agent_1:3.1+dfsg-8+deb10u3
```

133419 (1) - Debian DSA-4616-1 : qemu - security update 6

Slika 3: Primjer Nessus® modula (eng. plugin)

Kao što je prikazano na Slika 3 zaglavlje modula čine jedinstvena numerička oznaka (*eng. id*), zatim broj u zagradi koji nam govori na koliko različitih uređaja je Nessus® detektirao isti propust, te na kraju i naziv modula koji nam pobliže opisuje o kojoj vrsti ranjivosti se radi. Sam modul sastoji se od nekoliko cjelina koje kratko komentiramo u nastavku:

- *Synopsis* — jednom rečenicom dan je kratak opis modula, bilo da se radi o otkrivenoj ranjivosti ili informaciji o otkrivenom servisu
- *Description* — sadrži detaljan opis otkrivene ranjivosti. U opisu se najčešće navodi uzrok otkrivenog sigurnosnog propusta, način na koji ga je moguće iskoristiti te posljedice iskorištavanja sigurnosnog propusta

• *See Also*	poveznice na web sjedišta na kojima je moguće pročitati dodatne informacije o otkrivenoj ranjivosti, u slučaju da ponuđeni opis i rješenje nisu dovoljno detaljni
• *Solution*	sadrži opis rješenja otkrivenog sigurnosnog propusta
• *Risk factor*	daje informaciju o razini sigurnosnog rizika temeljenog na CVSS BaseScore-u
• *References*	dodatne reference za pronađeni sigurnosni propust (BugtraqID [6],CVE [7], XREF)
• *CVSS v.3.0 Base Score*	CVSS ili Common Vulnerability Scoring System je besplatan i otvoreni industrijski standard (*eng. open industry standard*) za procjenjivanje ozbiljnosti pronađenih ranjivosti na skali od 0 do 10, gdje 10 obilježava najozbiljnije
• *Exploitable with*	alati kojima je moguće iskoristiti pronađeni sigurnosni propust (Metasploit, CANVAS, Core Impact...)
• *Plugin Output*	prikazan je standardni izlaz modula te IP adrese svih uređaja na kojima je Nessus® otkrio sigurnosni propust. Ako je Nessus® otkrio neke specifičnosti vezane uz otkriveni propust (npr. inačica ranjivog programskog paketa, popis direktorija kojima je moguće pristupiti i sl.), iste će biti prikazane ispod navedene IP adrese

5 Otklanjanje pronađenih ranjivosti

Rezultate izvještaja provjere ranjivosti treba vrlo pažljivo i temeljito analizirati te poduzeti mjere s ciljem otklanjanja pronađenih ranjivosti. Polaznom točkom za otklanjanje pronađenih ranjivosti preporučujemo slijediti upute o uklanjanju koje se nalaze u ranije spomenutoj rubrici „*Solution*“. Nadalje, savjetujemo provjeriti i ugasiti servise koji se ne koriste ili za koje nema potrebe da budu dostupni s Interneta, odnosno korištenje vatrozida (eng. *firewall*) na uređaju. Također, preporučamo definirati pravila pristupa pojedinoj aplikaciji samo za računala koja imaju stvarnu potrebu pristupa toj aplikaciji - za svaku aplikaciju koja to omogućuje.

Preporučamo vam da sigurnosne ranjivosti kritičnog i visokog rizika otklonite što je prije moguće, ali također vam napominjemo da je, zbog korelacije pojedinih ranjivosti, potrebno otkloniti i ranjivosti srednjeg rizika. Naime, iskorištavanje nekoliko propusta srednjeg rizika može rezultirati jednakim posljedicama kao i prilikom iskorištavanja sigurnosnog rizika visoke razine rizika. Stoga, još jednom napominjemo da je svaku ranjivost potrebno pomno analizirati te ju otkloniti u što kraćem roku.

6 Literatura

1) OWASP – ranjivosti: https://owasp.org/www-community/vulnerabilities/ (srpanj, 2020.)

2) Wikipedia – ranjivosti: http://en.wikipedia.org/wiki/Vulnerability_%28computing%29 (srpanj, 2020.)

3) Informacije o Nessus-u® -u: https://www.tenable.com/products/nessus (srpanj, 2020.)

4) Wikipedija – *vulnerability scanner*: http://en.wikipedia.org/wiki/Vulnerability_scanner (srpanj, 2020.)

5) Informacije za CVSS3.1 Base Score – https://www.first.org/cvss/v3.1/specification-document (srpanj, 2020.)

6) Informacije za Bugtraq – http://en.wikipedia.org/wiki/Bugtraq (srpanj, 2020.)

7) Informacije za CVE – http://cve.mitre.org/ (srpanj, 2020.)