CARNET

Upute za tumačenje izvještaja provjere ranjivosti (Rapid7-Nexpose®)

CERT.hr-PUBDOC-2019-12-392

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 Nexpose® *vulnerability scanner*.

Nexpose® 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 Nexpose® 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. Nexpose® trenutno podržava više od 4000 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 generira se PDF izvještaj 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:

- kritične sigurnosne ranjivosti (eng. *Critical vulnerabilities*)
- sigurnosne ranjivosti visokog rizika (eng. *Severe vulnerabilities*)
- sigurnosne ranjivosti srednjeg rizika (eng. *Moderate vulnerabilities*)

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.

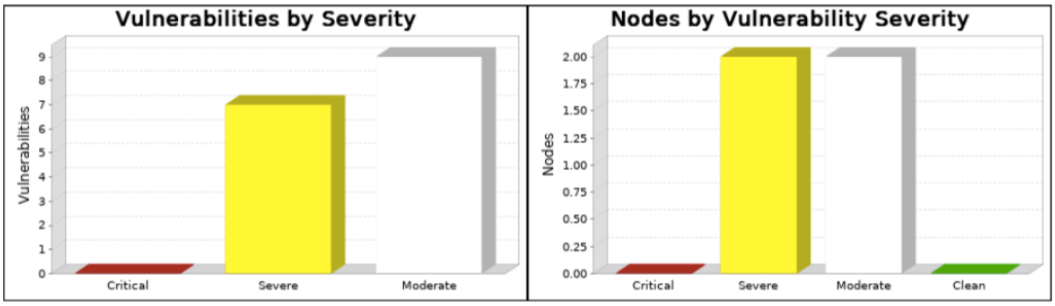
Izvještaj provjere ranjivosti sastoji se od nekoliko cjelina čiji sadržaj kratko komentiramo u nastavku.

4.1 Otkriveni sustavi (eng. *Discovered Systems*)

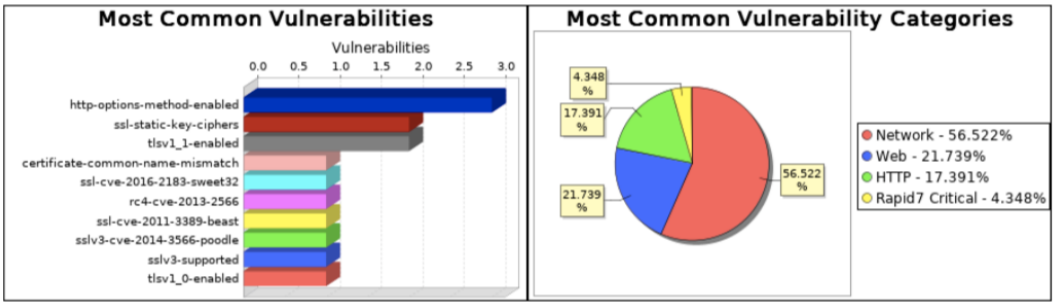
U ovo cjelini, dokument sadrži popis pronađenih računalnih sustava te tablični prikaz osnovnih informacija o svakom pojedinom pronađenom sustavu.

4.2 Kratak pregled (eng. *Executive Summary*)

Ova cjelina prikazuje sažete najbitnije informacije cjelokupnog procesa provjere ranjivosti. Kroz grafičke prikaze, prikazane su najbitnije informacije kao što su najčešće ranjivosti, ranjivosti po kategorijama i drugo. Ovaj dio izvještaja je lako čitljiv i ne tehničkim osobama te se lako dobije dojam sigurnosni sustava.



There were 16 vulnerabilities found during this scan. No critical vulnerabilities were found. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 7 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 9 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. No critical vulnerabilities were found on any of the systems. 2 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 2 systems. No systems were free of vulnerabilities.



Slika 1 Kratak pregled (eng. Executive Summary)

4.3 Procjena rizika (eng. *Risk Assessment*)

Ovaj dio izvještaja identificira sigurnosne rizike koji mogu utjecati na Vaše ključne radnje i imovinu. Ti se rizici kvantificiraju prema vjerojatnosti nastanka i potencijalnoj šteti ako se dogode. Kombinacijom čimbenika rizika, stvara se indeks rizika za svaki pronađeni sustav, omogućujući Vam da u skladu s time date prioritet svojim aktivnostima sanacije ranjivosti.

4.4 Otkrivene i potencijalne ranjivosti (eng. *Discovered and Potential Vulnerabilitis*)

U ovoj cjelini dokument sadrži detaljan izvještaj svih pronađenih ranjivosti poredani po prethodno navedenim kategorijama

Opis ranjivosti sadrži:

- *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
- *Affected Nodes* – prikazuje IP adresu ranjivog uređaja
- *References* – dodatne reference za pronađeni sigurnosni propust
- *Vulnerability Solution* – sadrži opis rješenja otkrivenog sigurnosnog propusta

4.2.4. TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)

Description:

The SSL protocol, as used in certain configurations of Microsoft Windows and browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (and other products negotiating SSL connections) encrypts data by using CBC mode with chained initialization vectors. This potentially allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. By supporting the affected protocols and ciphers, the server is enabling the clients in to being exploited.

Affected Nodes:

Affected Nodes:	Additional Information:
[redacted]	Negotiated with the following insecure cipher suites: SSL 3.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.0 ciphers: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHATLS_RSA_WITH_AES_256_CBC_SHA

References:

Source	Reference
CVE	CVE-2011-3389
URL	http://vnhacker.blogspot.co.uk/2011/09/beast.html

Vulnerability Solution:

There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and

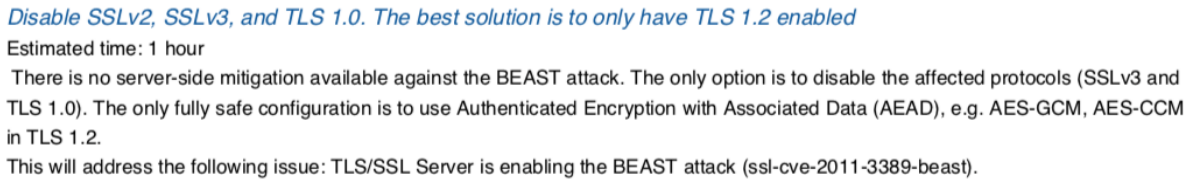
Slika 2 Detaljan prikaz pronađene ranjivosti

4.5 Otkriveni servisi (eng. *Discovered Services*)

U ovoj cjelini, dokument sadrži popis pronađenih omogućenih servisa (protokola). Uz kratak opis pojedinog protokola koji se koristi na Vašem sustavu, izvještaj definira glavne sigurnosne probleme vezane za taj servis kao i gdje je tokom provjere ranjivosti pronađena ranjivost vezana za taj servis.

4.6 Plan otklanjanja pronađenih ranjivosti (eng. *Remediation Plan*)

U ovoj cjelini, dokument sadrži informacije o pokrenutim javno dostupnim servisima. Uz kratak opis pojedinog servisa (protokola) koji se koristi na Vašem sustavu, izvještaj definira glavne sigurnosne probleme vezane za taj servis kao i gdje je tokom provjere ranjivosti pronađena ranjivost vezana za taj servis.


Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled
Estimated time: 1 hour
There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.
This will address the following issue: TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast).

Slika 3 Prijedlog otklanjanja pronađene ranjivosti

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 spomenutom poglavlju „*Remediation Plan*“. 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://www.owasp.org/index.php/Vulnerability (prosinac, 2019.)

2) Wikipedia – ranjivosti: http://en.wikipedia.org/wiki/Vulnerability_%28computing%29 (prosinac, 2019.)

3) Informacije o Nexpose® -u: https://www.rapid7.com/products/nexpose/ (prosinac, 2019.)

4) Nexpose®, rad s ranjivostima: https://nexpose.help.rapid7.com/docs/working-with-vulnerabilities (prosinac, 2019.)

5) Wikipedija – *vulnerability scanner*: http://en.wikipedia.org/wiki/Vulnerability_scanner (prosinac, 2019.)

6) Informacije za CVSS Base Score – http://www.first.org/cvss (prosinac, 2019.)

7) Informacije za Bugtraq – http://en.wikipedia.org/wiki/Bugtraq (prosinac, 2019.)

8) Informacije za CVE – http://cve.mitre.org/ (prosinac, 2019.)

7 Popis slika