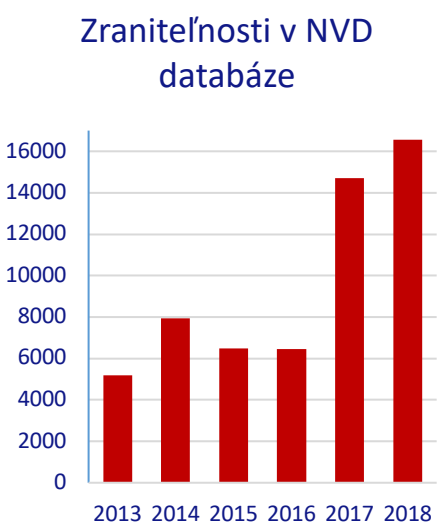
SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

NÁVOD NA OZNAMOVANIE ZRANITEĽNOSTÍ

#ÚVOD

National Institute of Standards and Technology (NIST) prevádzkuje National Vulnerability Database (NVD). Za rok 2018 evidoval naprieč všetkými existujúcimi softvérovými produktami a platformami spolu 16 555 zraniteľností, ktorým bol priradený kód CVE. Znamená to, že v priemere bolo objavených každý deň najmenej 45 zraniteľností rôznej kritickosti. Objavenie, oprava a zverejnenie zraniteľnosti by mali podliehať určitým pravidlám, aby sa čo najviac eliminovala možnosť zneužitia konkrétnej zraniteľnosti, čo môže mať následok nie len vo funkčnosti zraniteľného systému alebo služby, ale najmä priamy dopad na používateľov v podobe straty, pozmenenia alebo úniku dát, nedostupnosti služby alebo iných závažných skutočností.



Štyri dôvody existencie zraniteľností:

#1
Bezpečnosť je veľakrát v rozpore s tlakom na nové funkcie aplikácií a služieb a rýchlosťou vývoja a nasadenia. Benefity bezpečného dizajnu a s nimi spojená úspora sa pritom prejavujú až neskôr, počas prevádzky. Túto súvislosť však autori aplikácií často podceňujú.

#2
Vývoj softvéru kombinuje znalosti programovacieho jazyka, knižníc, databáz, komunikačných protokolov (voči iným aplikáciám, databázam, serverom, používateľovi) a súborových formátov. Získať a udržiavať si špičkové znalosti z najnovších bezpečnostných praktík vo všetkých týchto oblastiach je pre programátora extrémne náročné. Myslieť na všetky prípady a nedopustiť sa žiadnej chyby, aj keď ich programátor pozná, je prakticky nemožné.

#3
Aj keby programátor dodržal vo svojom vlastnom kóde všetky mysliteľné bezpečnostné odporúčania a neurobil žiadne chyby, občas je odhalená úplne nová kategória zraniteľností alebo sa zmení vonkajšie prostredie, následkom čoho treba prerobiť aplikáciu, aby sa novej situácii prispôsobila.

#4
Do aplikácií sú vnášané aj cudzie chyby z použitých externých knižníc a operačného systému. Tie môžu spôsobiť, že v aplikácii sa vyskytnú zneužiteľné zraniteľnosti aj napriek tomu, že jej autor dodržal všetky bezpečnostné zásady.

Tento návod obsahuje odporúčania Národného centra kybernetickej bezpečnosti SK-CERT týkajúce sa postupu pri oznamovaní zraniteľností. Je určený bezpečnostným výskumníkom, kybernetickým aktivistom, ale aj bežným občanom. Tento návod je vhodné použiť aj pri oznamovaní zraniteľností v produktoch a službách Národného bezpečnostného úradu a Národného centra kybernetickej bezpečnosti SK-CERT.

#ZRANITEĽNOSŤ

Všeobecne je zraniteľnosťou každá okolnosť, ktorá znižuje odolnosť voči hrozbám.

Zraniteľnosť je úmyselná alebo neúmyselná chyba softvérového produktu, hardvéru alebo procesu, ktorá umožňuje neautorizovaným osobám alebo procesom prístup k aktívam (dáta, softvér, hardvér, ľudia, ...), znemožňuje autorizovaný prístup k aktívam, či umožňuje neautorizovaným osobám a procesom vyhnúť sa detekcii.

Zneužitie zraniteľnosti znamená aj:

- # možnosť vykonať ľubovoľný kód (neautorizovaný, neplánovaný, škodlivý...)
- # získať administrátorské privilégiá alebo privilégiá inej používateľskej skupiny alebo užívateľa
- # zneprístupniť službu alebo produkt
- # získať neautorizovaný prístup k citlivým dátam na čítanie alebo ich modifikáciu

#CVE kód

Ak je zraniteľnosť produktu alebo služby odhalená, po procese oznámenia zodpovednému subjektu (najčastejšie výrobca alebo prevádzkovateľ) je zraniteľnosti pridelený CVE kód – Common Vulnerabilities and Explosures Code. Tento kód môže prideliť niektorý z participujúcich CSIRT tímov, Bug Bounty programov, výrobcov, bezpečnostných výskumníkov alebo organizácia MITRE ako primárna CVE číslovacia autorita. CVE kód slúži na centrálnu evidenciu všetkých známych zraniteľností.

#CVSS

Systém CVSS (Common Vulnerability Scoring System) je metrika, ktorá umožňuje porovnať závažnosť rôznych zraniteľností. CVSS skóre je konečným číslom od 0 do 10, vypočítaným pomocou exaktných vzorcov, zahŕňajúcich spôsob zneužitia, dopady na dôvernosť, integritu a dostupnosť a iné kritériá.

Metriku CVSS je možné použiť nielen na určenie závažnosti zraniteľnosti, ale aj na prioritizáciu jej riešenia, resp. odstránenia. Aktuálna verzia CVSS metriky (v 3.1) rozoznáva štyri kategórie zraniteľností:

SKÓRE	ZÁVAŽNOSŤ
0.1 – 3.9	Low (Nízka)
4.0 – 6.9	Medium (Stredná)
7.0 – 8.9	High (Vysoká)
9.0 – 10.0	Critical (Kritická)

CVSS možno vypočítať pomocou kalkulačky, ktorú nájdete na odkaze:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Metodiku CVSS verzie 3.1 si môžete prečítať na odkaze:
https://www.first.org/cvss/specification-document

#PREČO

#Prečo oznamovať zraniteľnosti?

Bezpečnosť každého systému je definovaná jeho najslabším článkom. Zraniteľnosti otvárajú útočníkom cestu do vnútra systému, k citlivým dátam, osobným údajom a vo veľa prípadoch aj k celkovému ovládnutiu napadnutého systému.

Ak by informácie o zraniteľnosti neboli oznámené autorovi softvéru a prevádzkovateľovi služieb, boli by tieto služby vystavené riziku útokov od strán, ktoré o tejto zraniteľnosti vedia. Ak by, naopak, bola informácia o zraniteľnosti verejne publikovaná predtým, než výrobca dostal šancu zraniteľnosť opraviť a záplatu distribuovať používateľom, mohlo by to viesť k panike a masovému zneužívaniu zraniteľnosti útočníkmi.

Zodpovedné koordinované oznámenie zraniteľnosti je najlepším spôsobom, ako zraniteľnosť odstrániť s minimom nežiadúcich dopadov. Zároveň poskytuje oznamovateľovi príležitosť získať uznanie odbornej verejnosti a prípadnú odmenu (Bug Bounty). CSIRT môže oznamovateľovi v prípade potreby poskytnúť anonymitu, alebo ho previesť všetkými krokmi procesu. Výrobcovi umožňuje včasná informovanosť o zraniteľnosti minimalizovať dopady na používateľov a predchádzať majetkovým a reputačným škodám.

Benefity pre oznamovateľa:

- # oznámením podľa pravidiel môže zabrániť zneužitiu zraniteľnosti nebezpečným útočníkom
- # pomôže postihnutému subjektu a zároveň aj používateľom zraniteľného systému alebo služby
- # trénuje svoje schopnosti v kybernetickej bezpečnosti

Benefity pre postihnutý subjekt:

- # dozvie sa o probléme, na ktorý môže ihneď reagovať a tak zabrániť škodlivým účinkom
- # dodržiavaním pravidiel zlepšuje svoje produkty a služby, ktoré ponúka svojim zákazníkom
- # buduje si dobré meno v bezpečnostnej komunite

ODPORÚČANÝ POSTUP PRE OZNAMOVATEĽA

Zraniteľnosť oznámiť Národnému centru kybernetickej bezpečnosti SK-CERT čo najskôr po jej odhalení, aby bolo minimalizované riziko zneužitia zraniteľnosti útočníkmi.
Na zachovanie dôvernosti odporúčame komunikáciu šifrovať prostredníctvom PGP.
Oznámenie zraniteľnosti musí obsahovať čo najpodrobnejší popis problému. Je možné uviesť aj návrh riešenia zraniteľnosti.
Odporúčame v oznámení uviesť podrobné kontaktné údaje aj spolu s uvedením možností zabezpečenej komunikácie (napr. PGP fingerprint).
SK-CERT môže oznamovateľovi pomôcť s ďalšími krokmi riešenia:
    * odborne posúdiť oznámenú zraniteľnosť.
    * prideliť CVE číslo pre zraniteľnosť.
    * identifikovať dotknuté subjekty a príslušné kontakty (výrobca, národné CSIRTy, zasiahnutí používatelia).
    * kontaktovať dotknuté subjekty či už s uvedením identity alebo zachovaním anonymity oznamovateľa.
Oznamovateľ môže určiť postihnutému subjektu lehotu na odstránenie zraniteľnosti, počas ktorej zraniteľnosť neoznámi verejne. Ak subjekt nereaguje na oznámenie a lehota uplynie, oznamovateľ môže zraniteľnosť oznámiť verejne. Dobrým zvykom je k oznámeniu zraniteľnosti pridať aj spôsoby riešenia alebo mitigácie zraniteľnosti. Štandardná lehota je 30 až 90 dní podľa povahy zraniteľnosti.

 # Oznamovateľ by sa mal v zraniteľnom systéme vyhnúť nasledujúcim činnostiam:
**   * inštalovať škodlivý kód**
**   * kopírovať, meniť alebo mazať dáta**
**   * robiť v systéme zmeny**
**   * opakovane sa prihlasovať do systému alebo zdieľať možnosť prihlásenia s tretími stranami**
**   * využívať iné spôsoby (napr. Brute Force) na hlbší prienik do systému**
 # Tieto činnosti sú protiprávne a môžu byť trestným činom alebo priestupkom.

ODPORÚČANIA PRE POSTIHNUTÝ SUBJEKT (VÝROBCA, VLASTNÍK, PREVÁDZKOVATEĽ ZRANITEĽNÉHO SYSTÉMU)

Spoločnosť by mala mať implementovaný:
    * proces oznamovania zraniteľností (proces by mal posúdiť každý oznámený problém a neobmedzovať sa len na vyššie ohodnotené zraniteľnosti)
    * proces prioritizácie a riešenia zraniteľností
    * proces oznamovania zraniteľností verejnosti
Odozva na každé oznámenie by mala byť rýchla a adekvátna oznámenej zraniteľnosti.
Riešenie zraniteľnosti by malo mať vysokú prioritu a jej oprava zaradená do najbližšej aktualizácie.
Riešenie by malo zahŕňať aj identifikáciu potenciálne zasiahnutých obetí a spôsob ich vyrozumenia.
Ak má byť zraniteľnosť oznámená verejnosti, spoločnosť určí dátum oznámenia a vyrozumie oznamovateľa, ak zraniteľnosť nenašla sama. Takisto po konzultácii s oznamovateľom zvolí vhodný kanál oznámenia zraniteľnosti komunite a širokej verejnosti.
Spoločnosť môže oznamovateľa za oznámenie zraniteľnosti odmeniť. Takisto môže „vypísať odmenu“ za nachádzanie zraniteľností vo svojich produktoch. Tento postup odporúčame, nakoľko vedie k zvýšeniu bezpečnosti produktov a služieb spoločnosti.
Oznámenie zraniteľnosti treba vnímať ako príležitosť na zlepšovanie produktov a šancu dozvedieť sa o zraniteľnosti skôr, než jej zneužitie spôsobí škody používateľovi, prevádzkovateľovi alebo výrobcovi produktu alebo služby. Preto odporúčame pristupovať k oznamovateľovi s vďakou ako k osobe, ktorá vám chce pomôcť - ako k priateľskému spolupracovníkovi. To, samozrejme, nevylučuje právne kroky v prípade, ak je postup oznamovateľa zjavne neetický či v rozpore so zákonom.

#AUTORITA

ZO STRANY KYBERNETICKEJ AUTORITY/AUTORÍT SA OČAKÁVA:

- # Národné kybernetické autority, v Slovenskej republike Národné centrum kybernetickej bezpečnosti SK-CERT, by mali vydávať štandardy a odporúčania v súvislosti s oznamovaním, riešením a oznamovaním zraniteľností verejnosti.
- # V prípade oznámenia zraniteľnosti kybernetickej autorite koordinovať postup s postihnutým subjektom a oznamovateľom.
- # V prípade potreby a v súlade s platnými právnymi predpismi zabezpečiť anonymitu oznamovateľa z dôvodu ochrany pred neoprávneným postihom alebo pred zastrašovaním zo strany výrobcu či prevádzkovateľa zraniteľného produktu alebo služby.
- # Podporovať oznamovanie zraniteľností budovaním bezpečnostného povedomia a motiváciou spoločností, bezpečnostných výskumníkov a iných subjektov.
- # Pri nahlásení zraniteľnosti, ktorá sa priamo týka kybernetickej autority, postupovať v súlade s odporúčaniami pre postihnutý subjekt.

#KONTAKTY NA NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI SK-CERT

SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Národný bezpečnostný úrad

Budatínska 30 | 851 06 Bratislava | Slovenská republika

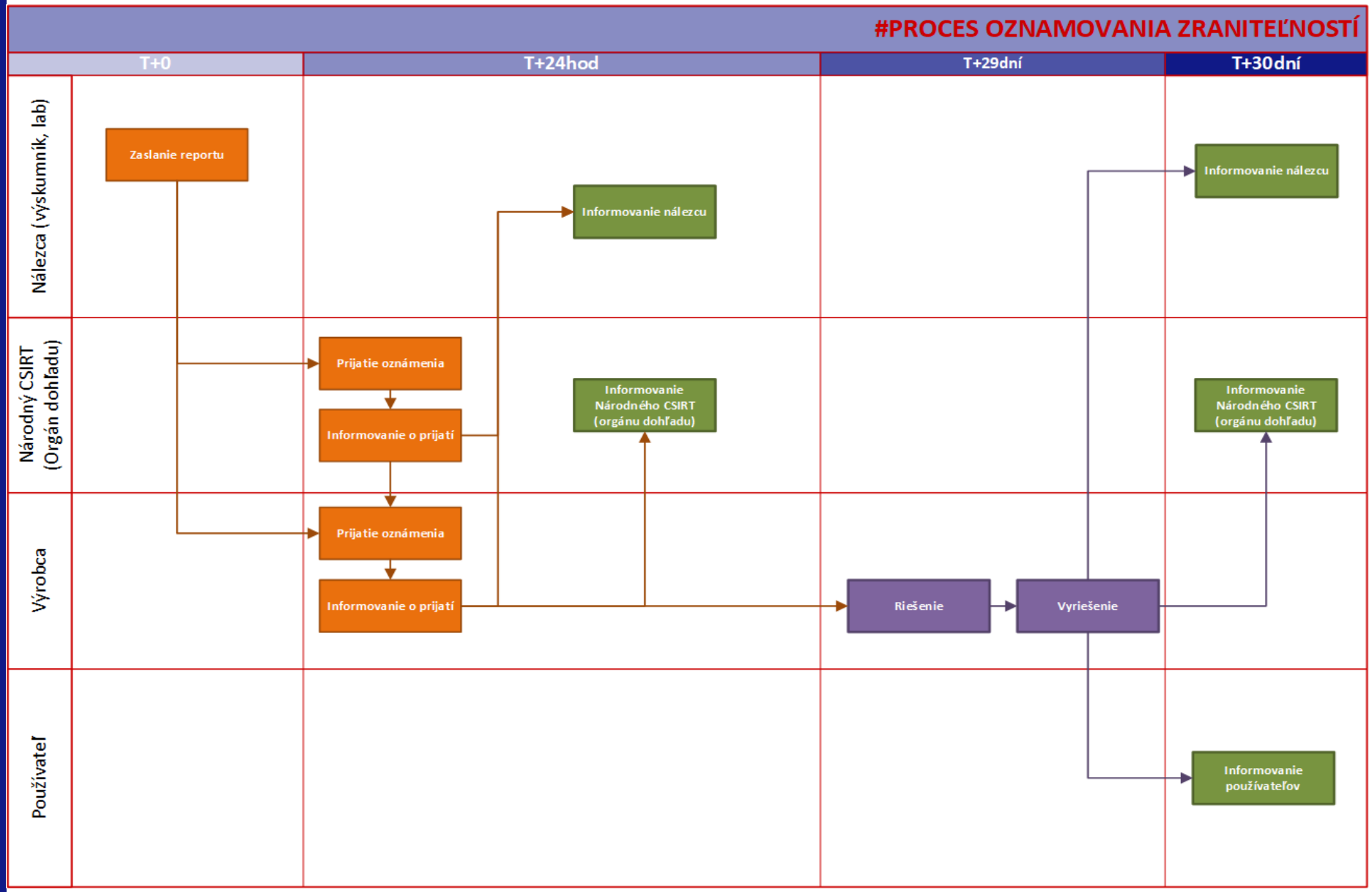
tel.: +421 2 6869 2915 | mob.: +421 903 993 706

e-mail: incident@nbu.gov.sk

PGP Fingerprint: D66E 619A E83A 8802 51A6 5AC7 CF74 96BD 1A1A 0ACD

web: https://www.sk-cert.sk | https://www.nbu.gov.sk

SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI



#O DOKUMENTE

Tento dokument vytvorilo a udržiava Národné centrum kybernetickej bezpečnosti SK-CERT Národného bezpečnostného úradu.

 # O NÁS

V súvislosti s určením Národného bezpečnostného úradu (ďalej len „úrad“) za ústredný orgán štátnej správy pre kybernetickú bezpečnosť úrad zriadil útvar **Národné centrum kybernetickej bezpečnosti SK-CERT (Slovak Computer Emergency Response Team)**. Útvar zabezpečuje národné a strategické aktivity v oblasti riadenia kybernetickej bezpečnosti, v oblasti analýzy hrozieb ale aj koordinácie riešenia bezpečnostných incidentov na národnej úrovni.

1. apríla 2018 nadobudol účinnosť zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorý vymedzuje úlohy, práva a povinnosti v oblasti kybernetickej bezpečnosti. Zákon zároveň určuje postavenie Národného bezpečnostného úradu ako Národnej jednotky CSIRT, pričom túto úlohu plní samostatný útvar Národné centrum kybernetickej bezpečnosti SK-CERT.

Tento dokument vznikol s podporou Národného centra kybernetickej bezpečnosti Holandska, ktoré vydalo niekoľko dokumentov ku koordinovanému oznamovaniu zraniteľností.

Viac o tomto dokumente a oznamovaní zraniteľností nájdete na:

https://www.sk-cert.sk/sk/oznamovanie-zranitelnosti/index.html

#REVÍZIE

VERZIA	DÁTUM	POZNÁMKA
1.0	04.10.2019	Prvá verzia dokumentu