Pravidlá pre oznamovanie zraniteľností zistených na informačných systémoch prevádzkovaných ÚVSR:

Čo je to zraniteľnosť:

Všeobecne je zraniteľnosťou každá okolnosť, ktorá znižuje odolnosť voči hrozbám. Zraniteľnosť v zmysle kybernetickej bezpečnosti 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.

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: 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 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.

- Zraniteľnosť zistenú na elektronických službách Úradu vlády Slovenskej republiky oznámte aj na adresu webmaster@vlada.gov.sk
- Na zachovanie dôvernosti odporúčame komunikáciu šifrovať prostredníctvom PGP.
- Oznámenie zraniteľnosti musí obsahovať čo najpodrobnejší popis problému. Je možné uviesť aj návrh riešenia zraniteľnosti, ak ho oznamovateľ má.
- 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).
  ⇒ 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.