Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS

UFCS – GESTIONE DELLE VULNERABILITÀ

Vulnerability Disclosure Management

Una guida per le organizzazioni e le imprese

01.02.2024

Indice

1 Introduzione

Se una persona interna o esterna scopre una falla di sicurezza nei sistemi o nei prodotti informatici della vostra organizzazione o impresa, dovrebbe poterlo segnalare immediatamente al servizio informatico competente della vostra organizzazione o impresa secondo un processo chiaramente definito.

Grazie a una procedura di notifica chiara e comprensibile, le organizzazioni e le imprese di tutte le dimensioni possono ottenere direttamente informazioni sulle vulnerabilità e dunque eliminarle in modo più rapido e mirato. Una procedura chiaramente definita mostra inoltre che l'organizzazione o l'impresa prende sul serio il tema della sicurezza e si sforza di migliorare costantemente i propri sistemi e i propri prodotti.

La presente guida dell'UFCS sulla divulgazione delle vulnerabilità («Vulnerability Disclosure») si rivolge alle organizzazioni e alle imprese per aiutarle a realizzare una procedura di notifica simile al loro interno. Tale procedura comprende le tre tematiche principali seguenti: comunicazione, direttive e «security.txt».

La guida si basa essenzialmente sullo standard internazionale per la divulgazione di vulnerabilità (ISO/IEC 29147:2018). Esso definisce le tecniche e le direttive applicabili alla ricezione delle segnalazioni delle vulnerabilità e alla pubblicazione delle informazioni sulla loro eliminazione. Lo standard ISO/IEC 29147:2018 è stato adottato il 3 maggio 2020 dal Comitato europeo di normazione («European Committee for Standardization, CEN»).

1.1 Obiettivi della divulgazione delle vulnerabilità

La divulgazione delle vulnerabilità consente da un lato di eliminare le falle di sicurezza, dall'altro di prendere decisioni più informate circa i rischi. Secondo lo standard ISO/IEC 29147:2018, la divulgazione delle vulnerabilità persegue vari obiettivi prioritari:

- ridurre i rischi eliminando le falle di sicurezza e informando gli utenti;
- ridurre al minimo i danni e i costi;
- fornire agli utenti le informazioni sufficienti per permettere loro di valutare i rischi dovuti alle vulnerabilità;
- definire le aspettative di tutte le parti interessate per agevolarne l'interazione e il coordinamento.

2 Struttura della guida

La presente guida verte su tre grandi tematiche che rivestono ciascuna un ruolo fondamentale nel processo di divulgazione delle vulnerabilità:

2.1 Comunicazione

2.1.1 Messa a disposizione di dati di contatto specifici

Una comunicazione rapida e immediata è decisiva per tutte la parti interessate.
Se collaboratori della vostra organizzazione o impresa, ricercatori di sicurezza informatica, hacker etici, l'UFCS o l'opinione pubblica sono a conoscenza di una vulnerabilità tecnica nella vostra organizzazione o impresa, è importante che tutti questi attori possano trovare rapidamente e contattare il servizio informatico competente per l'eliminazione di questa falla di sicurezza.

Spesso, però, questi dati (di contatto) specifici non sono disponibili. Spesso i rispettivi siti Internet riportano solo il numero del centralino o un indirizzo e-mail generale. Di conseguenza, chi inoltra la segnalazione deve rivolgersi a diverse persone spiegando più volte il problema prima di raggiungere l'interlocutore di riferimento e perdendo così tempo prezioso. Quando l'informazione perviene alla persona responsabile potrebbe già essere troppo tardi. Molte volte il servizio competente non sa nulla del problema perché le informazioni non vengono trasmesse o vengono ignorate. Questo è frustrante per chi ha trasmesso la segnalazione e irritante per l'organizzazione o l'impresa, che perde un'occasione per migliorare la propria cibersicurezza.

Per rimediare a questo problema, i dati di contatto dei responsabili informatici devono essere facili da reperire o bisognerebbe quantomeno definire un processo di segnalazione delle vulnerabilità all'interno dell'impresa. L'UFCS raccomanda di indicare i dati di contatto nella rubrica «Contatto» del sito Internet. Bisognerebbe inoltre registrare le opzioni di contatto nell'apposito file «security.txt» archiviato nel sito. (cfr. n. 2.3 «security.txt»).

2.1.2 Requisiti tecnici

Un indirizzo di posta elettronica appositamente creato o un modulo web permettono di garantire che tutte le informazioni concernenti una vulnerabilità giungano al servizio pertinente della vostra organizzazione o della vostra impresa.

Se la procedura di notifica adottata è basata sul web (ad. es. modulo web), il trasferimento dei

dati deve essere crittografato per esempio mediante il protocollo TLS (HTTPS). Analogamente, la comunicazione per posta elettronica dovrebbe ricorrere a soluzioni di crittografia e di firma come S/MIME o PGP. Le chiavi pubbliche necessarie devono essere registrate nel sito Internet ed essere accessibili.

Nella pagina Internet dell'UFCS è pubblicato un esempio di modulo web:

https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html

2.1.3 Processo

La presente guida definisce le quattro tappe del processo di trattamento delle vulnerabilità:

Ricezione della segnalazione:
Se ricevete una segnalazione relativa a una possibile vulnerabilità, sarebbe bene che ne accusiate la ricezione quanto prima, al più tardi entro sette giorni di calendario, ringraziandone l'autore. La risposta potrà essere generata automaticamente ma dovrà essere pertinente. Dovrebbe contenere un numero di tracciamento o un identificativo e dare informazioni provvisorie sullo stato di elaborazione del dossier.

Verifica:
In un secondo tempo si controlla e si verifica la vulnerabilità segnalata. In caso di grande afflusso delle segnalazioni, bisognerebbe procedere a una selezione sulla base della valutazione dei rischi relativi alle vulnerabilità. Alla fine di tale controllo vi raccomandiamo di informare l'autore della segnalazione in merito al risultato di questa prima valutazione.

Trattamento della vulnerabilità:
Durante il proseguimento del processo di trattamento delle vulnerabilità dovreste comunicare regolarmente con l'autore della segnalazione. La comunicazione dovrebbe contenere le informazioni seguenti:

- aggiornamenti dello status;
- nuove informazioni pertinenti;
- modifiche apportate ai progetti esistenti;
- calendario di pubblicazione.

Pubblicazione:
La comunicazione è l'elemento chiave. Dati di contatto facili da reperire e una comunicazione tempestiva, trasparente e rispettosa durante l'intero processo di trattamento delle vulnerabilità vanno a vantaggio dell'impegno e della motivazione degli autori delle segnalazioni.

2.2 Direttive

Grazie a direttive chiare potete precisare ciò che vi attendete dalla persona che vi segnala una vulnerabilità e ciò che questa persona ha il diritto di attendersi dalla vostra organizzazione o impresa. Gli autori delle segnalazioni possono così collaborare con voi in un quadro definito.

Secondo lo standard ISO/IEC 29147:2018, le direttive concernenti la divulgazione delle vulnerabilità devono obbligatoriamente abbordare determinati punti, mentre altri sono soltanto raccomandati:

- procedura di presa di contatto, ad esempio link o e-mail oppure modulo web **(obbligatoria)**;
- informazioni da menzionare nel rapporto sulla vulnerabilità, si veda anche l'allegato B dello standard ISO/IEC 29147:2018 **(raccomandate)**;
- requisiti relativi alla comunicazione **(raccomandati)**;
- ringraziamenti **(raccomandati)**;
- aspetti giuridici **(raccomandati)**.

Trovate un esempio di direttive sul sito Internet dell'UFCS:
https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html

Altri esempi di direttive sono contenuti nell'allegato A dello standard ISO/IEC 29147:2018.

2.3 security.txt

Lo standard «security.txt» consente di capire rapidamente chi contattare, all'interno di un'organizzazione o impresa, per tutto ciò che attiene alla sicurezza. Tale standard prescrive di registrare, nel repertorio «/.well-known» previamente definito sul server web che ospita il sito Internet, un file di testo denominato «security.txt». In questo file sono memorizzati almeno i dati di contatto dei responsabili della sicurezza del sito Internet oppure dell'organizzazione o impresa. È possibile aggiungervi link alle chiavi crittografiche, direttive sulla sicurezza e programmi speciali di divulgazione delle vulnerabilità o di ricompensa per chi scopre le vulnerabilità (programmi bug bounty).

Lo standard è stato ufficialmente riconosciuto nell'aprile 2022 come «RFC 9116», applicato in Internet da un numero sempre maggiore di imprese tecnologiche e organizzazioni governative di tutto il mondo.

Il file «security.txt» comprende indicazioni obbligatorie e indicazioni opzionali.

Dati	**Descrizione**	**obbligatori**	**opzionali**
Contatto	Link a un formulario web o indirizzo e-mail che consente di contattare l'organizzazione o l'impresa per qualsiasi domanda legata alla sicurezza. Aggiungete il prefisso «https://» o «mailto:» davanti a ogni URL.	X	

Data di scadenza	Data e ora a partire dalla quale bisognerà considerare obsoleto il contenuto del file «security.txt». Aggiornate regolarmente questo valore e riesaminate costantemente il vostro file.	X	
Lingua prescelta	Lista delle lingue, separate da virgole, parlate dal vostro servizio informatico. Potete specificare più di una lingua.		X
Opzioni di crittografia	Link alla chiave (ad es. PGP o S/MIME) che i ricercatori di sicurezza potranno utilizzare per comunicare con voi in tutta sicurezza.		X
Ringraziamenti	Link alla pagina Internet in cui l'organizzazione o l'impresa ringrazia i ricercatori di sicurezza che hanno segnalato un problema di sicurezza e che per questo motivo desiderano essere menzionati. Non dimenticate di indicare il prefisso «https://».		X
Link al file «security.txt»	Indirizzo URL del vostro file «security.txt». È importante indicarlo se il vostro file «security.txt» è munito di una firma digitale, perché in tal modo potrà recare la propria firma digitale anche lo spazio di archiviazione del file «security.txt».		X
Policy	Link a una direttiva che precisa come devono procedere i ricercatori di sicurezza per segnalarvi i problemi di sicurezza. Non dimenticate di indicare il prefisso «https://».		X
Offerte di lavoro	Link a tutte le offerte di lavoro legate alla sicurezza nella vostra impresa. Non dimenticate di indicare il prefisso «https://».		X

L'elenco non è esaustivo. Per informazioni più dettagliate, vogliate consultare lo standard RFC9116 (cfr. allegato).

2.2.1 Esempio di file «security.txt» (sito Internet dell'UFCS)

http://www.ncsc.admin.ch/.well-known/security.txt

```
# In the event that you have discovered a technical vulnerability in an IT system of the federal government,
# we encourage you to report it to the National Cyber Security Centre NCSC using the Coordinated Vulnerability
Disclosure program.
# We forward your request to the appropriate unit.
# If you are interested in participating in the NCSC bug bounty programs you can apply here:
https://www.bugbounty.ch/ncsc

Contact: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-
melden.html
Contact: mailto:incidents@ncsc.ch
Expires: 2024-12-31T23:59:59.000Z
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/pgp_ncsc_incidents.asc.dow-
nload.asc/NCSC_Incidents.asc
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/smime_incidents_ncsc_ch_22.cer.download.cer/
smime_incidents_ncsc_ch_22.cer
Preferred-Languages: en, de, fr, it
Canonical: https://www.ncsc.admin.ch/.well-known/security.txt
Policy: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-
melden/scope-and-rules.html
```

3 Link

ISO/IEC 29147:2018 Standard: Vulnerability disclosure
https://www.iso.org/standard/72311.html

ENISA - Coordinated Vulnerability Disclosure policies in the EU
https://www.enisa.europa.eu/about-enisa/about/it

IETF - RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure
https://www.ietf.org/rfc/rfc9116.pdf

OSCE learning: cyber/ICT security CBM 16: Coordinated Vulnerability Disclosure
https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about

UFCS - In primo piano: presunti ricercatori di sicurezza puntano a una ricompensa
https://www.ncsc.admin.ch/ncsc/it/home/aktuell/im-fokus/2022/wochenrueckblick_38.html