Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cancelleria federale CaF

Settore Trasformazione digitale e governance delle TIC (TDT)

18 ottobre 2022

Programma bug bounty eIAM

Rapporto

Sommario

1 Sintesi

eIAM è il sistema centrale di gestione degli accessi e delle autorizzazioni dell'Amministrazione federale per le applicazioni web e le applicazioni mobili native. Il Settore Trasformazione digitale e governance delle TIC (TDT) della Cancelleria federale quale responsabile del servizio eIAM, l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) quale gestore del sistema e il Centro nazionale per la cibersicurezza (NCSC) quale responsabile del programma bug bounty hanno svolto dal 30 agosto all'11 ottobre 2022 un programma privato bug bounty unitamente alla ditta Bug Bounty Switzerland AG.

Complessivamente sono state rilevate e segnalate 28 vulnerabilità, 14 delle quali sono state confermate come valide. Sono stati versati 5 700 franchi agli hacker etici che hanno partecipato al progetto.

Il numero complessivo delle vulnerabilità segnalate rientra comparabilmente nella media per un primo test con un gruppo di hacker etici. Non sono state rilevate falle di sicurezza critiche.

Il programma bug bounty eIAM è attualmente in pausa affinché siano valutate le esperienze raccolte e attuati eventuali adeguamenti organizzativi in vista di un suo possibile proseguimento.

2 Situazione iniziale

eIAM è il sistema centrale di gestione degli accessi e delle autorizzazioni dell'Amministrazione federale per le applicazioni web e le applicazioni mobili native. Si tratta quindi dell'infrastruttura centrale di accesso della Confederazione. Il servizio è utilizzato da oltre 1000 applicazioni tecniche. Mediante l'infrastruttura eIAM vengono eseguiti in media 550 000 accessi al giorno. Al Settore Trasformazione digitale e governance delle TIC (TDT) compete il controllo e la gestione dell'infrastruttura. L'Ufficio federale dell'informatica e della telecomunicazione (UFIT) ne assicura lo sviluppo e l'esercizio.

I programmi bug bounty costituiscono un metodo efficace ed economicamente vantaggioso per scoprire eventuali vulnerabilità dei sistemi informatici. Spesso oggi i test di sicurezza standardizzati non riescono più a rilevare lacune nascoste. Il progetto pilota svolto nella primavera 2021 in seno all'Amministrazione federale ha mostrato che, grazie a programmi bug bounty, è possibile rilevare e risolvere efficacemente le vulnerabilità nei sistemi e applicazioni TI. Sulla base di questi risultati, nell'agosto 2022 la Confederazione ha creato una piattaforma di programmi bug bounty[1].

Nei programmi bug bounty i cosiddetti «hacker etici» – che operano in un quadro definito e nel rispetto della legge – sono incaricati di individuare vulnerabilità nei sistemi informatici e nelle applicazioni di un'organizzazione. Per ciascuna vulnerabilità trovata, documentata e convalidata («bug») gli hacker vengono ricompensati («bounty») secondo la gravità della vulnerabilità sulla base di uno standard internazionale riconosciuto.

[1] L'Amministrazione federale acquisisce una piattaforma per i programmi bug bounty (admin.ch)

3 Esecuzione

Il Settore TDT della Cancelleria federale responsabile del servizio eIAM, l'UFIT quale gestore del sistema e il NCSC responsabile del programma bug bounty hanno svolto questa valutazione del sistema congiuntamente alla ditta Bug Bounty Switzerland AG.

Il programma bug bounty eIAM si è svolto dal 30 agosto all'11 ottobre 2022. Gli hacker etici ammessi al programma sono stati invitati specificatamente per questo programma bug bounty privato. L'esecuzione ha avuto luogo nell'ambiente di accettazione di eIAM, elaborato parimenti all'ambiente di produzione. Nell'ambiente di accettazione sono disponibili soltanto dati di test.

Inizialmente il sistema per la gestione degli account nonché diverse funzionalità di login (CH-Login, Harrods-Login, eIAM-Login e FED-Login) sono stati definiti e selezionati quali condizioni quadro («scope»). Dopo quattro settimane le condizioni quadro sono state estese a ulteriori funzionalità (gestione delegata e KeyCloak OIDC).

Il gruppo di hacker etici è stato circoscritto a professionisti noti all'NCSC o a Bug Bounty Switzerland AG e che si sono già distinti in altri progetti. Il numero degli hacker etici è stato aumentato da 9 a 32 nel corso del programma.

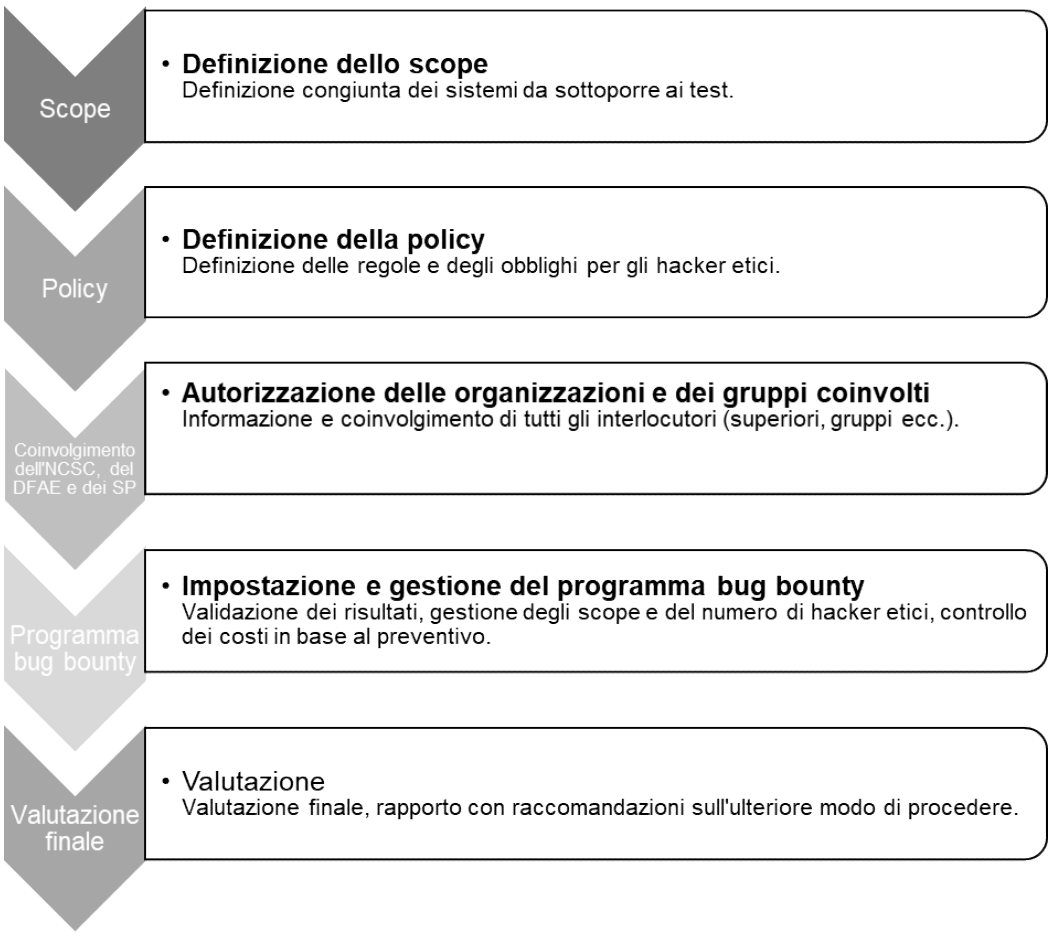
Le vulnerabilità sono state classificate sulla scala mondialmente riconosciuta CVSS[2] con livelli di criticità «basso», «medio», «elevato» o «critico». La scala consente una discussione obiettiva tra i servizi responsabili e gli hacker etici riguardo alla criticità e agli effetti generati dalle vulnerabilità. Una divergenza tra il grado di criticità segnalato e il grado di criticità convalidato non è inusuale e può essere motivato mediante i parametri specificati dalla scala.

Il team di sviluppo di eIAM ha definito le priorità per l'eliminazione delle falle convalidate sulla base delle seguenti regole:

- critico: eliminazione immediata
- elevato: eliminazione rapida
- medio: eliminazione mediante pianificazione delle release
- basso: eliminazione opzionale in base all'effetto generato

[2] Cfr.p. es. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Il programma bug bounty della Confederazione è stato eseguito con successo secondo la seguente procedura standard:

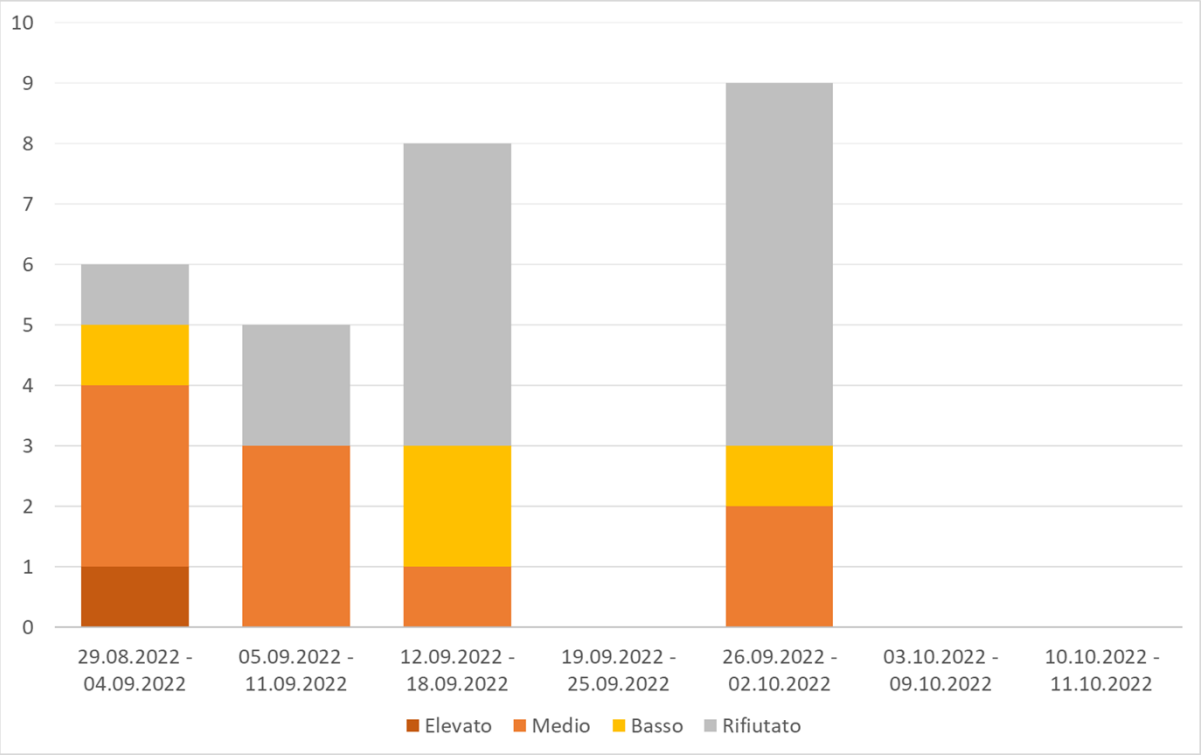


Il programma bug bounty di eIAM è attualmente in pausa affinché possano essere valutate le esperienze raccolte e attuati gli eventuali adeguamenti organizzativi necessari al suo proseguimento.

4 Risultati

Dal giorno di avvio del programma, il 30 agosto 2022 alle ore 09.00 al giorno della sua interruzione provvisoria, l'11 ottobre 2022 alle ore 23.59, sono state segnalate 28 vulnerabilità, 14 delle quali confermate come valide. I motivi per cui altre vulnerabilità segnalate sono state respinte erano principalmente riconducibili a doppioni nelle segnalazioni o a segnalazioni estranee alle condizioni quadro definite.

Il seguente grafico mostra la ripartizione settimanale delle segnalazioni:



Le lacune di sicurezza confermate sono state ripartite come segue:

	Critico	Elevato	Medio	Basso	Totale
Numero di vulnerabilità	**0**	**1**	**9**	**4**	**14**

La vulnerabilità con un grado di criticità «elevato» ha potuto essere colmata durante il programma. Le altre vulnerabilità sono confluite nella pianificazione delle prossime release.

La frequenza delle segnalazioni di vulnerabilità riscontrata all'inizio del programma riflette la situazione tipica che si presenta nelle prime esecuzioni di programmi bug bounty con nuove condizioni quadro da parte di hacker etici a causa delle regole competitive tra loro.

Particolarmente interessante si è rivelata la collaborazione tra gli hacker e i servizi TI operativi, responsabili dei sistemi e delle applicazioni. Grazie a una solida documentazione delle vulnerabilità individuate dagli hacker etici, i servizi responsabili hanno compreso il processo di rilevamento delle falle e hanno quindi avviato immediatamente l'analisi. Questa preziosa collaborazione fondata su una solida fiducia reciproca costituisce la base per la realizzazione di programmi bug bounty di successo.

5 Finanziamento

L’esecuzione del programma era stata organizzata nel quadro del bilancio operativo di eIAM. L’importo delle «bounty» (ricompense) versate ammonta a 5 700 franchi.

6 Conclusione

Le prime settimane di esecuzione del programma bug bounty di eIAM hanno mostrato che le vulnerabilità hanno potuto essere rilevate e risolte efficacemente. Dalla qualità e dal contenuto delle segnalazioni è emerso che questo metodo funge da complemento ad altri metodi a causa del fatto che gli hacker etici segnalano vulnerabilità non rilevabili mediante test di sicurezza usuali.