Policy pubblica coordinata per la divulgazione delle vulnerabilità.

Nice prende sul serio la sicurezza dei propri prodotti e servizi digitali. Se ritieni di avere individuato una vulnerabilità di sicurezza relativa a un prodotto o servizio Nice, ti invitiamo a segnalarcela. Questa policy spiega come inviare la segnalazione, quali informazioni possono aiutarci a valutarla e cosa puoi aspettarti da noi.

Come effettuare una segnalazione

1. Canale raccomandato: utilizza il modulo online per la segnalazione delle vulnerabilità disponibile nella pagina Nice dedicata alle segnalazioni di sicurezza. Il modulo può essere inviato senza indicare la tua identità. I campi che non conosci possono essere compilati con “non noto”.
2. Canale alternativo: invia un’e-mail a security@niceforyou.com utilizzando un oggetto chiaro, ad esempio: «Segnalazione di vulnerabilità – [prodotto o servizio]».
3. Non inserire dati personali non necessari o informazioni riservate di terzi. Se desideri ricevere aggiornamenti, indica un recapito affidabile.
4. Il modulo online e security@niceforyou.com confluiscono nel medesimo processo monitorato di ticketing. A ogni segnalazione sono assegnati un identificativo univoco e un timestamp di ricezione. Le informazioni per l’invio sicuro, compresa la chiave di cifratura ove applicabile, sono disponibili nella pagina di segnalazione e nel file security.txt pubblicato.

Informazioni da includere

1. prodotto o servizio interessato, oppure una descrizione sufficiente a identificarlo; modello, versione firmware/software, versione dell’applicazione o URL possono essere indicati se noti;
2. descrizione chiara della possibile vulnerabilità e, se noto, del potenziale impatto;
3. passaggi necessari per riprodurre il problema e, se disponibile, proof of concept; tali elementi sono utili ma non obbligatori se il segnalante non è in grado di fornirli;
4. condizioni necessarie per lo sfruttamento, inclusi vettore di attacco e privilegi richiesti, se noti;
5. eventuali informazioni che facciano ritenere che la vulnerabilità sia già attivamente sfruttata; se non è possibile determinarlo, seleziona o indica “non noto/non osservato”.

Cosa puoi aspettarti da Nice

1. Ci proponiamo di confermare la ricezione entro 3 giorni lavorativi. La conferma contiene l’identificativo del caso e attesta esclusivamente la ricezione, non la validazione della vulnerabilità segnalata.

2. Ci proponiamo di fornire una prima valutazione o un aggiornamento entro 10 giorni lavorativi.
3. Se l'analisi rimane aperta e hai fornito un recapito, ci proponiamo di comunicare un aggiornamento almeno ogni 30 giorni, salvo che ragioni legali, di sicurezza o di riservatezza impediscano di condividere determinate informazioni.
4. Questi termini costituiscono obiettivi di servizio relativi alla comunicazione con il segnalante e non sostituiscono né modificano i termini di legge applicabili a Nice.

Divulgazione concordata.

Ti chiediamo di concedere a Nice un tempo ragionevole per analizzare e, ove opportuno, correggere il problema segnalato prima di renderlo pubblico. Cercheremo di concordare con te la divulgazione, tenendo conto della gravità della vulnerabilità, della disponibilità delle misure correttive, della tutela degli utilizzatori e degli obblighi di legge applicabili. Ove opportuno e con il tuo consenso, Nice potrà riconoscere pubblicamente il tuo contributo.

Ricerca di sicurezza condotta in buona fede

Se conduci la ricerca di sicurezza in buona fede e nel rispetto di questa policy, Nice non intraprenderà né sosterrà azioni legali nei tuoi confronti esclusivamente in relazione a tale attività. Questo impegno si applica unicamente ai sistemi e alle attività rientranti nell'ambito della policy e nella sfera di competenza di Nice. Non vincola soggetti terzi e non autorizza condotte illecite o eccedenti i limiti indicati di seguito.

Regole per la ricerca

1. effettua test esclusivamente su prodotti, account, dispositivi o sistemi di tua proprietà o per i quali disponi di un'autorizzazione espressa;
2. evita violazioni della riservatezza e riduci al minimo l'accesso a dati personali o informazioni confidenziali;
3. interrompi il test e informaci tempestivamente se accedi a dati non necessari a dimostrare la vulnerabilità;
4. non conservare, modificare, cancellare, scaricare, copiare, divulgare o utilizzare dati appartenenti a Nice, agli utilizzatori o a terzi, salvo le informazioni minime strettamente necessarie a documentare la vulnerabilità;
5. non mantenere accessi persistenti, non effettuare attività di ingegneria sociale, minacce o estorsioni, non interrompere i servizi e non eseguire test denial-of-service o volumetrici;
6. non sfruttare la vulnerabilità oltre quanto strettamente necessario per dimostrarla; e
7. concedi un tempo ragionevole per l'analisi e la correzione prima della divulgazione pubblica.

Ambito di applicazione

La policy si applica ai prodotti Nice con elementi digitali che si trovano nel periodo di supporto dichiarato, inclusi firmware, software, applicazioni mobili e servizi cloud associati, nonché ai siti web e ai servizi digitali gestiti direttamente da Nice. Le segnalazioni relative a prodotti non più supportati possono comunque essere inviate e saranno valutate caso per caso, senza che ciò comporti un impegno a rendere disponibile un aggiornamento correttivo.

Attività escluse

1. sistemi, prodotti o servizi gestiti esclusivamente da terzi, salvo che Nice ne abbia espressamente autorizzato l'inclusione;
2. attacchi fisici, ingegneria sociale, phishing o attacchi contro dipendenti, collaboratori, clienti o fornitori;
3. attacchi DoS o DDoS e test che possano compromettere disponibilità o prestazioni;
4. test automatizzati che generino traffico eccessivo o interferiscano con il normale funzionamento del servizio;
5. accesso, modifica, distruzione, conservazione, estrazione o divulgazione di dati oltre quanto strettamente necessario per dimostrare la vulnerabilità; e
6. test su prodotti, account, dispositivi o sistemi che non siano di tua proprietà e per i quali non disponi di autorizzazione.

Segnalazioni relative a componenti di terzi

Se la segnalazione riguarda un componente di terzi integrato in un prodotto Nice, inviala comunque a Nice. Valuteremo il problema e, ove necessario, ci coordineremo con il produttore, fornitore o manutentore del componente secondo il processo interno di gestione delle vulnerabilità.

Nessun impegno relativo a bug bounty

Questa policy non istituisce un programma di bug bounty e non attribuisce alcun diritto a pagamenti, premi o altre forme di compenso. Qualsiasi riconoscimento o premio dovrà essere espressamente concordato per iscritto con Nice.

Dati personali

I dati personali trasmessi con la segnalazione saranno trattati esclusivamente nella misura necessaria a ricevere, valutare, analizzare e gestire la segnalazione, comunicare con il segnalante, proteggere Nice e i suoi utilizzatori e adempiere agli obblighi di legge. L'informativa privacy applicabile ai sensi del Regolamento (UE) 2016/679 è disponibile nella pagina dedicata alle segnalazioni di sicurezza.