SCOPERTA E DIVULGAZIONE DELLE VULNERABILITÀ

Versione 1.3- Novembre 2022

Introduzione

Sylvania ritiene che la sicurezza, la privacy e la protezione dei propri clienti siano una delle sue principali priorità. Progettiamo e realizziamo prodotti e servizi con la migliore qualità e affidabilità possibile. Nonostante i nostri sforzi per implementare le migliori misure di sicurezza possibili, è possibile che nei nostri prodotti e servizi siano presenti delle vulnerabilità.

Questo documento descrive la politica di Sylvania per la ricezione di segnalazioni relative a potenziali vulnerabilità di sicurezza nei suoi prodotti e servizi, le procedure dell'azienda per la gestione di una segnalazione e la prassi standard dell'azienda per quanto riguarda l'informazione ai clienti delle vulnerabilità verificate.

Tutti sono incoraggiati a segnalare le vulnerabilità identificate, indipendentemente dal tipo di servizio o di prodotto. Ricercatori, partner, clienti o qualsiasi altra fonte sono invitati a segnalare le vulnerabilità riscontrate.

Ambito di applicazione

Questa politica si applica ai seguenti sistemi e servizi:

- sylvania-lighting.com
- https://comnet.sylvania-lighting.com
- http://lightingportal.feilosylvania.com/
- SylSmart Energy (energy.sylvania-lighting.com)
- - Applicazione mobile SylSmart Home
- - Applicazione mobile SylSmart Standalone
- - Applicazione mobile SylSmart Connected e applicazione web (https://connected.sylvania-lighting.com/)
- - Applicazione mobile Solution Sylvania
- - Applicazione web SylSmart City (city.sylvania-lighting.com / city.sylvania-latam.com)
- - Applicazione mobile SylSmart City

Nota per i ricercatori: Tutti i servizi non espressamente elencati sopra sono esclusi dal campo di applicazione e non sono autorizzati per la sperimentazione.

Linee guida

Vi chiediamo di:

- Notificare prima e il più presto possibile a Feilo Sylvania la scoperta di un problema di sicurezza reale o potenziale.

- Fare ogni sforzo per evitare violazioni della privacy, degrado delle prestazioni del sistema, degrado dell'esperienza dell'utente, interruzione dei sistemi di produzione e distruzione o manipolazione dei dati.

- Utilizzare gli exploit solo nella misura necessaria a confermare la presenza di una vulnerabilità.

- Non utilizzare un exploit per compromettere o estrarre i dati, stabilire l'accesso alla riga di comando e/o la persistenza, o utilizzare l'exploit per "fare rotta" verso altri sistemi.

- Una volta accertata l'esistenza di una vulnerabilità o la presenza di dati sensibili (tra cui informazioni di identificazione personale, informazioni finanziarie o informazioni proprietarie o segreti commerciali di qualsiasi parte), **è necessario interrompere il test, informare immediatamente Feilo Sylvania e non divulgare tali dati a nessun altro.**

- Dare a Feilo Sylvania un tempo ragionevole per risolvere il problema.

- Non utilizzare test di negazione del servizio di rete (DoS o DDoS) o altri test che compromettono l'accesso o danneggiano un sistema o i dati.

Se queste linee guida vengono seguite, non verranno intraprese azioni legali nei confronti di chi scopre e segnala una vulnerabilità.

Segnalazione di una vulnerabilità

Il metodo preferito per contattare Feilo Sylvania in merito a una vulnerabilità reale o potenziale dei suoi prodotti o servizi è l'invio di un'e-mail a:

info@sylvania-lighting.com.

Al fine di elaborare in modo efficiente la segnalazione della vulnerabilità, ci aspettiamo un rapporto ben scritto in inglese contenente le seguenti informazioni:

- Ora e data della scoperta

- Applicazione mobile utilizzata

- Sistema operativo mobile

- Modello di computer e dettagli del sistema operativo

- Numero di modello del dispositivo e indirizzi MAC/UUID associati

- Modello e numero del prodotto utilizzando, se possibile, la nomenclatura del fornitore

- URL, informazioni sul browser, compresi il tipo e la versione e l'input richiesto per riprodurre la vulnerabilità;

- Descrizione tecnica - fornire le azioni eseguite e il risultato nel modo più dettagliato possibile, comprese le schermate,

- Codice di esempio - se possibile, fornire il codice utilizzato nei test per creare la vulnerabilità;

- Informazioni di contatto della parte segnalante - i migliori dettagli di contatto.

- Piano/i di divulgazione - piano attuale di divulgazione;

- Valutazione della minaccia/rischio e valutazione della gravità - contiene i dettagli delle minacce e/o dei rischi identificati, compreso un livello di rischio (minore, maggiore, critico).

- Informazioni rilevanti sui dispositivi collegati se la vulnerabilità emerge durante l'interazione.

Si prega di non includere dati personali nelle segnalazioni, ad eccezione di quelli necessari per contattare l'utente in linea con la conformità al GDPR.

La partecipazione a questo meccanismo di segnalazione non conferisce alcun diritto alla proprietà intellettuale di Feilo Sylvania o di terzi.

Elaborazione del rapporto - Fasi successive

Una volta ricevuta la segnalazione, Feilo Sylvania si impegnerà a confermare la ricezione di tutte le segnalazioni inviate entro sette giorni.

La segnalazione verrà elaborata nel nostro sistema di tracciamento dei problemi. La valutazione della gravità della segnalazione verrà presa in considerazione e assegnata a discrezione di Feilo Sylvania e un membro appropriato del team contatterà l'utente per dare seguito alla segnalazione.

Per garantire la riservatezza, vi invitiamo a criptare tutte le informazioni sensibili che ci inviate via e-mail. Feilo Sylvania garantirà un dialogo aperto per discutere i problemi e vi terrà informati in ogni fase dell'indagine.

Feilo Sylvania ha piena discrezione nel determinare se accettare una segnalazione in base al livello di gravità o al contenuto della segnalazione stessa.

Feilo Sylvania vi ringrazia per l'assistenza fornita nell'identificazione di una vulnerabilità, per migliorare i nostri prodotti e servizi e per contribuire a una comunità più sicura.

Tutti gli aspetti di questo processo sono soggetti a modifiche senza preavviso e ad eccezioni specifiche. Non è garantito un particolare livello di risposta per alcun problema specifico o gruppo di problemi.

Non è prevista alcuna ricompensa finanziaria per le vulnerabilità segnalate.