Metodologie, strumenti e sicurezza dei dati “by design” affidabili per il test dinamico di componenti hardware e software potenzialmente vulnerabili e insicuri.

Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components

TOPIC ID: HORIZON-CL3-2022-CS-01-02
Ente finanziatore: Commissione europea Programma Horizon Europe

Obiettivi ed impatto attesi: Metodologie e strumenti affidabili per l’analisi e la verifica avanzata e il test dinamico di componenti hardware e software potenzialmente vulnerabili e insicuri richiedono buone pratiche per la sicurezza dei sistemi, con particolare attenzione agli strumenti di sviluppo del software, alle metriche di sicurezza informatica e alle linee guida per prodotti e servizi sicuri per tutta la loro durata. È necessaria una metodologia olistica, che integri metodi di runtime per il monitoraggio e l’applicazione e metodi di design-time per l’analisi statica e la sintesi dei programmi, che consenta di costruire sistemi sicuri con le più forti garanzie formali possibili. Il firmware dei dispositivi, le implementazioni dei protocolli e degli stack di comunicazione, i sistemi operativi (OS), le interfacce di programmazione delle applicazioni (API) che supportano l’interoperabilità e la connettività di diversi servizi, i driver dei dispositivi, il software di backend per il cloud e la virtualizzazione, nonché il software che implementa diverse funzionalità di servizio, sono alcuni esempi di come il software fornisca l’essenza dei sistemi e degli oggetti intelligenti (in rete). Le questioni relative alla catena di fornitura, compresa l’integrazione di software e hardware, devono essere considerate in modo appropriato.

Saranno finanziate attività di ricerca e sviluppo per sviluppare strumenti ibridi, agili e ad alta garanzia in grado di automatizzare i processi di valutazione, strumenti di responsabilità per i risultati delle verifiche e gli aggiornamenti e ambienti di virtualizzazione leggeri e isolati in grado di ispezionare e orchestrare in modo sicuro le apparecchiature in architetture hardware e software eterogenee. Inoltre, è necessario sviluppare KPI, metriche, procedure e strumenti per la certificazione dinamica della sicurezza dell’implementazione e della sicurezza scalabile, dal livello di chip a quello di software e di servizio. Può anche includere metodi di test come il fuzzing guidato dalla copertura e l’esecuzione simbolica.

La partecipazione delle PMI è fortemente incoraggiata. In questo tema l’integrazione della dimensione di genere (analisi del sesso e del genere) nei contenuti della ricerca e dell’innovazione non è un requisito obbligatorio.

Si prevede che i progetti contribuiscano ai seguenti risultati attesi:
• Controllo efficace dell’accesso ai componenti del sistema e gestione degli aggiornamenti affidabili.
• Modellazione delle proprietà di sicurezza e privacy e quadri di riferimento per la convalida e l’integrazione nel processo di test.

• Processo integrato per il test, la verifica formale, la convalida e la considerazione degli aspetti di certificazione (comprese le potenziali sinergie con il quadro di certificazione della cybersecurity dell'UE, come stabilito dalla legge sulla cybersecurity dell'UE).
• Strumenti che garantiscano che i componenti di terze parti e open source siano privi di vulnerabilità, punti deboli e/o malware.
• Sicurezza dei dati "by design", ad esempio attraverso blocchi crittografici sicuri
• Strumentazione e comunicazione sicura con i componenti del sistema per i test dinamici.
• Metodi e ambienti per la codifica sicura by-design e by-default e per la costruzione di hardware e software sicuri.
• Procedure di audit efficaci per i test di cybersecurity.
• Metodi o procedure per rendere sicure le catene di fornitura
• La proposta deve fornire indicatori appropriati per misurare i progressi e l'impatto specifico.

Criteri di eleggibilità: Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
-essere soggetti giuridici (enti pubblici o privati) avere sede in uno dei Paesi ammissibili, ovvero Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) Paesi non UE:
• Paesi SEE elencati
• Paesi in via di adesione,
I beneficiari e gli enti affiliati devono iscriversi al Registro dei partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà loro richiesto di caricare documenti che dimostrino lo status giuridico e l'origine.

Si applicano le seguenti eccezioni: Alcune attività, derivanti da questo tema, possono comportare l'utilizzo di background classificati e/o la produzione di risultati sensibili dal punto di vista della sicurezza (EUCI e SEN). Si rimanda alle relative disposizioni della sezione B Sicurezza - Informazioni classificate e sensibili dell'UE degli Allegati generali.

Schema di finanziamento: Contributo UE previsto per progetto
La Commissione ritiene che un contributo UE compreso tra 3 e 5 milioni di euro consentirebbe di affrontare adeguatamente questi risultati. Tuttavia, ciò non preclude la presentazione e la selezione di una proposta che richieda importi diversi.
Budget indicativo
Il budget totale indicativo per il tema è di 17,30 milioni di euro.
Tipo di azione Azioni di ricerca e innovazione Condizioni di ammissibilità Le condizioni sono descritte nell'Allegato generale B.

Scadenza: 16 novembre 2022 17:00:00 ora di Bruxelles

Ulteriori informazioni:
wp-6-civil-security-for-society_horizon-2021-2022_en.pdf (europa.eu)