AWS Nitro System API e Rivendicazioni di Sicurezza

Amazon Web Services, Inc.
Versione 1.0 - 11 aprile 2023

Preparato da
John Redford
Xiang Wen Kuan

Preparato per
Amazon Web Services

1 Sintesi

Sinossi

Nell'ultimo trimestre solare del 2022, Amazon Web Services (AWS) ha incaricato NCC Group di condurre una revisione del design architetturale del AWS Nitro System, con particolare attenzione alle rivendicazioni specifiche fatte da AWS circa la sicurezza delle API del Nitro System. La programmazione ed esecuzione di tale analisi è stata protratta durante il primo trimestre solare del 2023.

Di seguito è riportata una descrizione del Nitro System, in forma abbreviata rispetto alla documentazione pubblica[1]:

> AWS Nitro System è una combinazione appositamente realizzata di design di server, processori di dati, componenti per la gestione del sistema e firmware specializzato che costituisce le fondamenta di tutte le istanze EC2 lanciate a partire dall'inizio del 2018. I tre componenti chiave del Nitro System sono:
>
> - Schede Nitro Specifiche: dispositivi hardware appositamente progettati da AWS che forniscono il controllo generale del sistema e la virtualizzazione di input/output (I/O) indipendentemente dalla scheda principale di sistema con CPU e memoria.
> - Chip di sicurezza Nitro: basato su un hardware "root of trust", permette un processo di avvio sicuro per l'intero sistema, così come la capacità di offrire istanze bare metal, ed una difesa approfondita che protegge il server da modifiche non autorizzate del firmware di sistema.
> - Hypervisor Nitro: un hypervisor, volutamente ridotto al minimo e simile ad un firmware, progettato per fornire un forte isolamento delle risorse e prestazioni quasi indistinguibili da un server bare metal.

AWS ha effettuato diverse dichiarazioni circa la sicurezza con cui il Nitro System è progettato al fine di impedire ai dipendenti AWS di accedere ai dati dei clienti. Tali dichiarazioni sono elencate nella sezione Dichiarazioni di questo report.

Il Nitro System è stato progettato con lo scopo di garantire gli obiettivi di sicurezza trattati nelle suddette dichiarazioni fornendo un'infrastruttura di amministrazione, gestione e monitoraggio generale del sistema che opera dal livello hardware fino al provisioning, all'implementazione ed alla fine del ciclo di vita dei sistemi. AWS non dispone di metodi di accesso alternativi ai sistemi host Nitro EC2. Tale livello di attenzione ai dettagli, combinato con l'appropriato allineamento agli obiettivi di sicurezza attraverso pratiche aziendali sostenibili e realizzabili, ha consentito ad AWS di progettare un sistema capace di supportare solidamente le dichiarazioni circa la sicurezza e la privacy dei clienti.

Riguardo il design del Nitro System, NCC Group non ha riscontrato lacune che contraddicessero suddette affermazioni circa la sicurezza. Ogni design comporta dei compromessi, ed AWS ha optato per un design in cui l'impatto di una compromissione da parte di un utente malevolo è paragonabile ad un guasto hardware su piccola scala.

Logistica del progetto

L'ambito dell'analisi ha riguardato la verifica di una serie di dichiarazioni di sicurezza relative alla progettazione delle API amministrative di Nitro, così come i processi di sviluppo ed amministrativi che si occupano di creare e gestire le API Nitro. Gli operatori AWS utilizzano le API Nitro per eseguire una serie di attività ben definite. Questo ha riguardato lo sviluppo e l'implementazione degli elementi software del Nitro System, l'infrastruttura utilizzata e le procedure per la creazione e l'implementazione di un ambiente Nitro System.

1. Il design di sicurezza di AWS Nitro System https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html.

L'ambito della valutazione realizzata da NCC Group ha incluso:

- La API del Nitro System, le sue chiamate, funzionalità, i suoi processi di sviluppo ed implementazione e gli elementi dell'infrastruttura di supporto richiesti.
- Il ruolo degli operatori AWS autorizzati ad accedere alla API del Nitro System.
- Dipendenti AWS diversi dagli operatori, compresi gli sviluppatori di Nitro System ed il personale incaricato di gestire ed assegnare ruoli ai dipendenti.
- Revisione del Nitro System e del suo ecosistema con il fine di garantire che non fossero presenti o richiesti sistemi alternativi per design.

I seguenti elementi sono stati esclusi dalla valutazione:

- Valutazione generale dei servizi del piano di controllo (control-plane) EC2.
- Valutazione dell'hypervisor Nitro, del firmware Nitro e del software Nitro su schede Nitro.
- Valutazione delle schede Nitro.
- Valutazione dell'ambiente fisico e dei controlli di sicurezza fisica.

Metodologia di valutazione

La valutazione è stata effettuata in gran parte tramite interviste con il team di sviluppo di AWS Nitro e tramite l'accesso alla documentazione fornita da AWS. NCC Group ha realizzato colloqui con diversi ingegneri esperti del team Nitro, incluso l'ingegnere capo. Tali colloqui hanno trattato l'origine e gli obiettivi di progettazione del sistema, così come le sue caratteristiche ed i suoi vincoli operativi. Le informazioni sono inoltre state fornite sotto forma di documenti e tramite condivisione dello schermo con il fine di consentire a NCC Group di raggiungere una comprensione approfondita circa la sicurezza del Nitro System. La documentazione fornita ha trattato un grande numero di dettagli interni del progetto.

La valutazione non include una revisione approfondita circa l'implementazione di componenti specifici così come test pratici o di convalida tecnica. La valutazione delle dichiarazioni di sicurezza di AWS si è basata sulla capacità del design del Nitro System, così come valutato ed analizzato, nel fornire i mezzi che permettessero di rispettare le dichiarazioni stesse. Essendo la seguente un'analisi a livello di design, il mancato rispetto di una delle suddette dichiarazioni di sicurezza da parte del design comporterebbe che tale dichiarazione non è stata presa in considerazione.

Limitazioni del progetto

Questo progetto rappresenta una valutazione puntuale delle API del Nitro System. Le minacce alla sicurezza e le tecniche di attacco evolvono rapidamente, pertanto, i risultati di questa valutazione non intendono rappresentare una validazione dell'adeguatezza delle attuali misure di sicurezza contro minacce future. Inoltre, le dichiarazioni di NCC Group si riferiscono al sistema così come fornito durante la finestra temporale di valutazione e non forniscono alcuna garanzia in merito ad eventuali modifiche tecniche o deviazioni future nella politica. Sebbene il processo di avvio e l'interazione sicure delle schede Nitro siano stati un fattore di analisi, la sicurezza di questi sistemi in presenza di un attaccante fisico è stata rimandata ad una successiva attività di analisi o esclusa dall'ambito di applicazione.

Questa revisione si basa sulle dichiarazioni rilasciate del personale AWS e sui documenti di design del prodotto così come sono stati presentati a NCC Group. Sebbene AWS abbia fornito un supporto adeguato a tale riguardo, NCC Group non può attestare l'accuratezza delle informazioni o delle conclusioni associate o se l'implementazione corrisponde al design. Qualsiasi dichiarazione circa le funzioni del Nitro System si riferisce al suo design.

2 Progettazione di Nitro System

Introduzione

Per diversi mesi NCC Group ha realizzato una revisione del design architetturale del Nitro System, comprensivo di discussioni ed analisi, con aggiuntive pianificazioni e revisioni. L'obiettivo della revisione ha consistito nel determinare se l'architettura di Nitro System fosse in grado di soddisfare le affermazioni di sicurezza fatte da AWS. Il team di consulenza ha considerato il sistema dal punto di vista degli "operatori AWS", ovvero persone con accesso non pubblico all'ambiente, così come degli sviluppatori del Nitro System e di altri dipendenti di AWS.

L'analisi ha stabilito che tali API sono l'unico mezzo attraverso il quale gli operatori AWS possono interagire con gli host di istanze, dal momento che non ci sono ulteriori soluzioni per connettersi, accedere od ottenere altri tipi di accesso privilegiato. Inoltre, è stato constatato che nessun altro dipendente di AWS diverso dagli operatori AWS può utilizzare queste API.

Obiettivi di progettazione di Nitro System

Privilegio minimo

Il design di Nitro System aderisce al principio del privilegio minimo. Questo implica non permettere:

- Accesso ai dati dei clienti.
- Accesso per eseguire comandi o codice arbitrari.
- Personalizzazione di un'istanza con patch o versioni software uniche.
- Migrazione di dati o memoria di archiviazione ad un'altra istanza o ambiente.
- Attività non registrate.
- Procedure di emergenza per aggirare o rimuovere le protezioni di sicurezza.

Il design del Nitro System è stato considerato essere in linea con i requisiti essenziali degli ambienti al fine di gestire eventi su piccola scala di perdita di disponibilità, per esempio guasti hardware o incidenti. Il potenziale impatto di un abuso da parte di un utente malevolo avrebbe infatti un impatto paragonabile ai sopracitati eventi.

Ridondanza e Zero Trust

I componenti del Nitro System sono progettati per eseguire controlli di sicurezza ridondanti e stratificati. Il design garantisce che l'autenticazione e l'autorizzazione vengano verificate più volte e che siano necessarie diverse fasi per lo sviluppo ed implementazione di modifiche software. Gli host dell'istanza sono progettati per verificare in modo indipendente gli adeguati controlli di accesso prima di eseguire qualsiasi azione richiesta.

Confidenzialità ed integrità

L'intero design dell'ambiente include stretti controlli crittografici e di firma. L'architettura generale del Nitro System garantisce che tutte le comunicazioni dello stesso siano criptate in modo sicuro e che tutti i componenti dei Nitro System distribuiti siano firmati e validati. Per ridurre la possibilità di compromissione delle chiavi che proteggono le comunicazioni e gli aggiornamenti software, il design garantisce che le root of trust si trovino in sistemi protetti che non sono basati su livelli meno stringenti di controllo degli accessi per la gestione della sicurezza.

Ispezione e monitoraggio

Tutte le chiamate API del Nitro System vengono registrate in un ambiente CloudWatch sicuro con differenti livelli di controlli di accesso. I log vengono costantemente monitorati per l'identificazione di richieste o di modelli di attività considerati sensibili al fine di chiamare l'attenzione umana su tali sistemi. Tale monitoraggio, ed il coinvolgimento umano, vengono regolarmente testati, realizzando in aggiunta efficaci esercizi interni di "red teaming".

Incentivi di Design

Questi sono in linea con gli incentivi propi di AWS e dei suoi dipendenti. In alcuni ambienti, si crea naturalmente una gerarchia di accesso, con un numero limitato di amministratori che hanno accesso completo a molti sistemi corporativi, includendo spesso sistemi che controllano l'accesso ad altri sistemi. In ogni caso, i dipendenti AWS non hanno alcun motivo per avere tale accesso ai dati dei clienti. Ottenere tale accesso è infatti contrario agli obiettivi aziendali. Il design del Nitro System, così come il suo sviluppo ed implementazione, supportano l'incentivo per i dipendenti a non avere alcun modo di accedere ai dati dei clienti. Anche i processi interni del personale AWS che definiscono l'identità dei dipendenti riflettono e supportano questi incentivi.

Documentazione pubblica del Nitro System

Vari dettagli circa il design del Nitro System sono accessibili pubblicamente attraverso diverse piattaforme.

- Il design di sicurezza del AWS Nitro System.
  https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Modello di verifica del codice di avvio da parte dei data center AWS.
  https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:InForce 2019: vantaggi di sicurezza dell'architettura Nitro (SEP401-R).
  https://www.youtube.com/watch?v=kN9XcFp5vUM

3 Dichiarazioni

Dichiarazioni sul design di sicurezza del prodotto

AWS dichiara che gli host del Nitro System in ambiente di produzione aderiranno ad una politica esplicita di protezione della privacy dei dati dei clienti secondo le seguenti affermazioni:

1. Non esiste alcun meccanismo che consenta ad un dipendente di un fornitore di servizi cloud di accedere all'host sottostante.
2. Nessuna API amministrativa può accedere ai contenuti dei clienti sull'host sottostante.
3. Non esiste alcun meccanismo che consenta ad un dipendente di un fornitore di servizi cloud di accedere ai contenuti dei clienti archiviati su istanze di archiviazione di massa e volumi EBS criptati.
4. Non esiste alcun meccanismo che permetta ad un dipendente di un fornitore di servizi cloud di accedere ai dati criptati trasmessi sulla rete.
5. L'accesso alle API amministrative richiede sempre l'autenticazione e l'autorizzazione.
6. L'accesso alle API amministrative viene sempre registrato.
7. Gli host possono eseguire solo software testato e firmato, distribuito da un servizio di distribuzione autenticato ed autorizzato. Nessun dipendente di un fornitore di servizi cloud può distribuire codice direttamente sugli host.

Analisi delle dichiarazioni

1. Non esiste alcun meccanismo che consenta ad un dipendente di un fornitore di servizi cloud di accedere all'host sottostante.

Per design, i sistemi non espongono alcun meccanismo in grado di fornire l'accesso ad una shell o a qualsiasi altro meccanismo simile per l'esecuzione di comandi arbitrari. Non esiste alcun modo per abilitare o implementare un simile meccanismo. Allo stesso modo non esistono meccanismi speciali o esterni che permettono tale azione.

Analisi: NCC Group ritiene che l'architettura del Nitro System supporti pienamente questa affermazione. Non vi è alcuna indicazione che un dipendente di un fornitore di servizi cloud possa ottenere tale accesso od un accesso equivalente a qualsiasi host.

2. Nessuna API amministrativa può accedere ai contenuti dei clienti sull'host sottostante

Le API amministrative non svolgono alcuna attività per accedere o rivelare i contenuti dei clienti. Non esistono API che possano causare lo spostamento dei contenuti in un'altra posizione da cui è possibile accedervi. Non esistono API in grado di ridurre o rimuovere le protezioni sul contenuto dei clienti.

Analisi: NCC Group ritiene che l'architettura del Nitro System supporti pienamente questa affermazione. Le API amministrative non possono accedere al contenuto dei clienti sull'host sottostante. Questa funzionalità non esiste.

3. Non esiste alcun meccanismo che consenta ad un dipendente di un fornitore di servizi cloud di accedere ai contenuti dei clienti archiviati su istanze di archiviazione di massa e volumi EBS criptati.

La API amministrativa non include alcuna funzionalità che possano dare accesso ai contenuti dei clienti sull'istanza di archiviazione di massa. Non è possibile utilizzare la API per creare condizioni che permettano ciò. Gli elementi di archiviazione di massa delle istanze sono tutti criptati a riposo, così come i volumi EBS.

I volumi di archiviazione di massa EBS non criptati continuano ad esistere sotto scelta del cliente.

Analisi: NCC Group ritiene che l'architettura del Nitro System supporti pienamente questa affermazione. Non esiste alcun meccanismo mediante il quale un dipendente di un fornitore di servizi cloud possa accedere ai contenuti dei clienti archiviati su istanze host o in volumi EBS criptati.

4. Non esiste alcun meccanismo che permetta ad un dipendente di un fornitore di servizi cloud di accedere ai dati criptati trasmessi sulla rete.

La crittografia utilizzata per proteggere i dati relativi a Nitro ed altri metodi crittografici gestiti da AWS utilizzano algoritmi appropriati ed una gestione sicura delle chiavi. Il protocollo TLS 1.2 viene utilizzato per negoziare connessioni criptate. Le chiavi utilizzate direttamente dall'hardware Nitro sono archiviate in uno storage criptato, localmente protetto da un chip TPM a prova di manomissione. Tutte le comunicazioni amministrative tramite API e le comunicazioni gestite da AWS sono criptate in modo sicuro. AWS utilizza versioni del protocollo e varianti di algoritmo sicure e, se necessario, può migrare rapidamente a versioni più recenti.

Analisi: NCC Group ritiene che l'architettura di Nitro System supporti pienamente questa affermazione. Non esiste alcun meccanismo che consenta ai dipendenti dei fornitori di servizi cloud di accedere alle chiavi di crittografia o di disabilitare la crittografia delle comunicazioni.

5. L'accesso alle API amministrative richiede sempre l'autenticazione e l'autorizzazione.

Le API amministrative richiedono che le richieste contengano un bearer token che fornisca dati di autenticazione ed autorizzazione. Questi token vengono generati e forniti a un operatore autorizzato in base alla sua identità ed ai diritti di accesso ad esso associati. I token garantiscono l'accesso solo alle risorse per le quali sono stati emessi e scadono in un breve periodo di tempo. I diritti di accesso sono descritti dall'associazione di gruppi di operatori con API e set di risorse gestite specifici. I diritti di accesso sono limitati dalle quote sulle risorse interessate in un determinato periodo di tempo.

Gli stessi dati di configurazione dei diritti vengono verificati rapidamente e non sono eccessivamente complessi, in questo modo gli utenti non dispongono di diritti eccessivi o inappropriati. I dati di configurazione dei diritti di accesso sono definiti con il servizio del fornitore di token e seguono le stesse procedure di peer review e controllo delle modifiche.

Analisi: NCC Group ritiene che l'architettura del Nitro System supporti pienamente questa affermazione. Il sistema di bearer token implementato impedisce ad un utente malevolo di riutilizzare il token al di fuori del contesto autorizzato. I tempi di scadenza dei token sono sufficientemente lunghi da evitare problemi in caso di interruzione del servizio di emissione, ma sufficientemente brevi da limitarne l'uso improprio. L'individuazione della configurazione dei diritti di accesso con il codice per il sistema che fornisce i bearer token garantisce che entrambi abbiano la stessa protezione procedurale contro le alterazioni malevole. Le quote impediscono che qualsiasi abuso di accesso autorizzato influisca su un numero elevato di sistemi.

6. L'accesso alle API amministrative viene sempre registrato.

Tutti gli eventi di accesso, inclusa l'autenticazione o l'autorizzazione non riuscita delle richieste, verranno registrati immediatamente in un flusso di log CloudWatch dedicato creato e gestito dal team di sviluppo di AWS Nitro. Questi eventi vengono costantemente monitorati per rilevare eventuali attività o schemi di attività significativamente insoliti o sospetti.

Analisi: NCC Group ritiene che l'architettura di Nitro System supporti pienamente questa affermazione. Il processo di monitoraggio è configurato per identificare le richieste che possono indicare un abuso da parte di un agente malevolo o usi inappropriati delle API amministrative.

7. Gli host possono eseguire solo software testato e firmato, distribuito da un servizio di distribuzione autenticato ed autorizzato. Nessun dipendente di un fornitore di servizi cloud può distribuire codice direttamente sugli host.

La protezione dell'integrità del software ed i meccanismi di aggiornamento automatico dell'ambiente Nitro sono presenti sin dal momendo della fabbricazione. Il processo attraverso il quale i sistemi si avviano, acquisiscono l'identità ed eseguono funzioni di caricamento e gestione del software ad alto livello, è protetto sin da questo momento. È funzionalmente possibile riportare un componente Nitro allo stato di sicurezza iniziale. Da tale condizione, l'identità può essere assegnata in ambienti di produzione o non di produzione. Grazie ai controlli presenti sia nei componenti Nitro che negli ecosistemi, non è possibile spostare un componente in un altro ecosistema.

Analisi: NCC Group ritiene che l'architettura di Nitro System supporti pienamente questa affermazione. Le procedure e le pratiche utilizzate per sviluppare ed autorizzare il software non consentono ad alcun agente malevolo, anche se provvisto di accesso di AWS Operator o sviluppatore Nitro, di iniettare funzionalità non autorizzate nel sistema. Gli incentivi di tutte le persone autorizzate sono allineati al fine di prevenire che ciò accada.

4 Documenti analizzati

I seguenti documenti sono stati esaminati durante questa analisi.

Documentazione pubblica AWS

I documenti sotto riportati sono disponibili al pubblico e se ne consiglia la lettura per una più completa comprensione del Nitro System.

- Il design di sicurezza di AWS Nitro System.
  https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Modello di verifica del codice di avvio da parte dei data center AWS.
  https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:InForce 2019: vantaggi di sicurezza dell'architettura Nitro (SEP401-R).
  https://www.youtube.com/watch?v=kN9XcFp5vUM

Documentazione interna AWS

I documenti interni AWS elencati di seguito sono stati conservati in un ambiente AWS di sola lettura, senza realizzarne alcuna copia.

- **Documento sui controlli Nitro**: documentazione completa del design del Nitro System che tratta i controlli per impedire l'accesso da parte di un operatore al contenuto dei clienti. Tale documento include una panoramica dettagliata del Nitro System e dei suoi componenti, una descrizione della trusted computing base (TCB), una descrizione del funzionamento delle API Nitro, modelli di minaccia ed altro.
- **Nitro Security Design**: una prima versione di documento di design che trattava gli obiettivi e i vincoli di progettazione del Nitro System.
- **Infrastruttura a chiave pubblica EC2** - Documentazione sull'infrastruttura a chiave pubblica che fornisce le basi del rapporto di fiducia tra i componenti interni di EC2.
- **Contenuto dei Bearer Token**: documentazione specifica circa struttura dei bearer token utilizzati dal Nitro System.
- **Nitro Pipeline**: documentazione sull'agente di orchestrazione utilizzato per le distribuzioni del software Nitro. La Nitro Pipeline è il ponte tra gli strumenti standard di Amazon, il servizio di test ed altri servizi e strumenti EC2. Alcune parti di questo documento sono state offuscate.