Report del test

Rapporto sul test di sicurezza effettuato da un ente indipendente

Storage di archivio di backup immutabile Object First

Ottobre 2024

Aggiornamento sulla sicurezza

Object First si impegna a soddisfare gli standard di settore sulla sicurezza informatica per il suo prodotto di punta Ootbi (Out-of-the-box Immutability), che costituisce una destinazione di archiviazione "secure by design" per i dati di backup Veeam. Gli esperti di sicurezza migliorano continuamente l'hardening del prodotto e noi ci affidiamo regolarmente a società terze che effettuano test indipendenti per garantire la sicurezza di Ootbi per impostazione predefinita.

Ci siamo avvalsi dell'esperienza di NCC Group, un team di esperti di sicurezza informatica, per condurre test di penetrazione completi sul dispositivo Ootbi e sul relativo software per identificare e risolvere rischi non ancora individuati. Questo documento fornisce una sintesi dei risultati di NCC e informazioni importanti sulla sicurezza della tecnologia Ootbi di Object First.

Conclusioni di NCC

L'applicazione Ootbi è progettata per proteggere da qualsiasi violazione di dati o violazione da malware di un cliente Object First: anche se tutti i segreti del cliente, incluse le credenziali dell'amministratore e le credenziali del bucket, dovessero essere noti all'aggressore, quest'ultimo non potrebbe comunque modificare i dati memorizzati all'interno di un'appliance Ootbi.

-NCC Group, Ootbi Product Security Assessment, 31 luglio 2024

Com’è stata condotta la valutazione?

NCC Group ha incaricato due team di esperti (uno focalizzato sul codice sorgente software e l’altro su dispositivi di test di penetrazione pronti per la produzione) per valutare il dispositivo Ootbi e il codice sorgente nell’arco di 54 giorni in due cicli di test. Nel secondo ciclo di test, NCC ha convalidato che tutti i principali problemi di sicurezza identificati nel primo ciclo sono stati risolti. Sono stati approfonditi molti aspetti di Ootbi, inclusi:

- Servizi Web API S3: API frontali utilizzate da Veeam e altri sistemi per creare bucket e oggetti di archiviazione.
- Interfaccia utente di gestione: Console amministrativa basata sul Web per configurare bucket, criteri e gestire complessivamente il dispositivo.
- Server Ootbi di Object First: La soluzione on premises che consente alle aziende di mantenere backup immutabili di bucket di archiviazione.

Nota: gli attacchi che richiedono accesso fisico sono stati esclusi da questa valutazione.

Chi è NCC Group?

NCC Group è un’azienda globale di cyber e software resilience che opera in diversi settori, aree geografiche e tecnologie.

Tra gli altri servizi, fornisce consulenza globale ad imprese tecnologiche, produttori, istituti finanziari, fornitori di infrastrutture nazionali cruciali, rivenditori e amministrazioni su come proteggere le aziende da interruzioni impreviste e garantire la sicurezza, la protezione e la disponibilità continua delle loro applicazioni business-critical.

Risultanze e rimedi

Nel primo ciclo di test sono stati rilevati 20 problemi in totale, che sono stati risolti dal team tecnico di Object First prima del secondo ciclo di test. NCC ha rilevato che tutti i problemi tranne uno sono stati risolti (19/20). Il problema restante è stato valutato “a basso rischio” e non rappresenta una minaccia per la sicurezza nell’ambiente di lavoro corrente.

Di seguito è riportato un elenco completo dei risultati che NCC ha rilevato durante il primo ciclo di test, il relativo livello di rischio valutato e lo stato di risoluzione corrente dopo il secondo ciclo di test.

Problema	Rischio	Stato
Focus del test: **AWS API**		
L'applicazione ignora i nomi di servizio durante l'autorizzazione	Alto	Risolto
Limiti delle risorse non supportati per IAM API	Medio	Risolto
Limiti delle risorse non supportati da **s3:CreateBucket**	Medio	Risolto
Controlli delle autorizzazioni errati per **s3:CreateBucket**	Medio	Risolto
L'applicazione accetta parametri non firmati	Basso	Risolto
Nel confronto di firma tempo-variante mancano informazioni	Basso	Risolto
Focus del test: **API di gestione**		
Inserimento di comando del sistema operativo che genera esecuzione di codice remoto	Critico	Risolto
Comandi esterni eseguiti come comandi shell	Medio	Risolto
Gestione delle password non sicura	Medio	Risolto
L'aggiornamento della password utente di sistema non richiede una nuova autenticazione	Basso	Risolto
Riferimento a oggetti diretti non sicuro che genera un controllo dell'account arbitrario	Basso	Risolto
Focus del test: **Ootbi Server**		
Credenziali predefinite deboli	Alto	Risolto
Password proxy scritta nei registri	Medio	Risolto
Credenziali proxy incluse nel bundle di supporto	Medio	Risolto
Il server SSH consente l'inoltro TCP	Basso	Risolto
Il server SSH consente l'autenticazione della password	Basso	Risolto
L'autenticazione locale/SSH non supporta MFA	Basso	Non affrontato*
Focus del test: **Web UI**		
Download di bundle di supporto non autenticato	Medio	Risolto
Controlli di sicurezza lato client per whitelist IP	Basso	Risolto
Controlli della cache HTTP non sicuri	Basso	Risolto

*SSH è disabilitato per impostazione predefinita e viene visualizzato un avviso quando abilitato.

Resilienza dei dati Zero Trust

Anche gli esperti di NCC concordano con Object First sull'importanza di implementare strutture Zero Trust come parte dell'architettura di backup. Il quadro di riferimento Zero Trust Data Resilience è un modello che tutte le imprese possono utilizzare per ipotizzare uno stato di violazione e applicare i principi di Zero Trust, per garantire un rapido ripristino da un attacco, indipendentemente dal software di protezione dei dati o dallo storage scelto.

Valutate se il vostro fornitore si preoccupa di far testare i propri prodotti da terze parti per continuate a garantire che i vostri dati, indipendentemente da dove risiedono, utilizzino l'immutabilità in modalità di conformità (compliance mode) come parte della soluzione di archiviazione.

Cosa succede dopo?

Object First si impegna a soddisfare gli standard di settore sulla sicurezza informatica e i nostri team di ricerca, sviluppo e supporto sono focalizzati a garantire che Ootbi sia sicuro per impostazione predefinita. Collaboriamo regolarmente con aziende di test di terze parti indipendenti e condividiamo apertamente i risultati con la community. Ci impegniamo a portare avanti questo focus su sicurezza e trasparenza e restiamo saldi nella nostra dedizione alla tutela dei dati di backup Veeam.