Test Report

Independent Security Test Report

Object First Immutable Backup Storage Appliance

October, 2024

Security Update

Object First is committed to meeting IT security industry standards for its flagship product Ootbi (Out-of-the-box Immutability), which serves as a secure-by-design storage target for Veeam backup data. Security experts continuously improve the hardening of the product, and we regularly engage with independent, third-party testing firms for validation that Ootbi is secure-by-default.

We employed the expertise of the NCC Group, a team of cybersecurity experts, to conduct comprehensive penetration tests on the Ootbi appliance and its software to identify and address undiscovered risks. This paper provides a summary of NCC's findings and important security information about Object First's Ootbi solution.

NCC's Final Takeaway

The Ootbi application is designed to protect against any data breach or malware infestation of an Object First customer: even if all of the customer's secrets, including administrator credentials and bucket credentials, are known to the attacker, the attacker still cannot modify data stored within an Ootbi appliance.

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

How Was the Assessment Conducted?

The NCC Group had two teams of experts (one focused on software source code and the other focused on penetration testing production-ready devices) to evaluate the Ootbi appliance and the raw source code over 54 days during two rounds of testing. In the second round of testing, NCC validated that all major security issues identified in the first round had been resolved. They delved into many aspects of Ootbi, including:

- S3 API Web Services: Front-facing API used by Veeam and other systems to create buckets and store objects.
- Management User Interface: Web-based administrative console to set up buckets, configure policies, and generally manage the device.
- Object First Ootbi Server: The on-premises solution that enables companies to retain immutable backups of storage buckets.

Note: Attacks requiring physical access were considered out-of-scope for this engagement.

Who is NCC Group?

NCC Group is a global cyber and software resilience business operating across multiple sectors, geographies and technologies.

Among other services, they advise global technology firms, manufacturers, financial institutions, critical national infrastructure providers, retailers and governments on how to protect organizations from unforeseen disruptions and ensure their business-critical software applications and source code are safe, secure and always available.

Discoveries and Remediations

A total of 20 issues were detected in the first round of testing, which were addressed by the Object First engineering team before the second round of tests. NCC found that all but one of the issues were fixed (19/20). The remaining issue was deemed “low risk” and not a security threat in the current functional environment.

What follows is a complete list of the findings NCC recorded during the first round of testing, their assessed level of risk, and their current fixed status after the second round of testing.

Issue	Risk	Status
Test Focus: **AWS API**		
Application disregards service names during authorization	High	Fixed
Resource constraints not supported for IAM API	Medium	Fixed
Resource constraints not supported by **s3:CreateBucket**	Medium	Fixed
Incorrect permission checks for **s3:CreateBucket**	Medium	Fixed
Application accepts unsigned parameters	Low	Fixed
Time-variant signature comparison leaks information	Low	Fixed
Test Focus: **Management API**		
OS command injection leading to remote code execution	Critical	Fixed
External commands executed as shell commands	Medium	Fixed
Unsafe password handling	Medium	Fixed
System user password update does not require re-authentication	Low	Fixed
Insecure direct object reference leading to arbitrary account takeover	Low	Fixed
Test Focus: **Ootbi Server**		
Weak default credentials	High	Fixed
Proxy password written to logs	Medium	Fixed
Proxy credentials included in support bundle	Medium	Fixed
SSH server allows TCP forwarding	Low	Fixed
SSH server allows password authentication	Low	Fixed
Local/SSH authentication does not support MFA	Low	Unaddressed*
Test Focus: **Web UI**		
Unauthenticated support bundle download	Medium	Fixed
Client-side security controls for IP whitelist	Low	Fixed
Insecure HTTP caching controls	Low	Fixed

*SSH is disabled by default, and a warning is displayed when enabled.

Zero Trust Data Resilience

The experts at NCC also agreed with Object First on the importance of implementing Zero Trust frameworks as part of the backup architecture. The Zero Trust Data Resilience framework is a model all organizations can use to assume a breached state and apply Zero Trust principles to ensure rapid recovery from an attack regardless of the data protection software or storage stack you choose.

Evaluate whether your vendor is taking the time to have 3rd party agencies penetration test their products and continue to ensure that your data, no matter where it resides, is utilizing immutability in compliance mode as part of the storage stack.

What Comes Next?

Object First is committed to meeting IT security industry standards, and our research, development and support teams are focused on ensuring Ootbi is secure-by-default. We regularly engage with third-party, independent testing firms, and openly share those results with the community. We pledge to continue this focus on security and transparency, and will remain steadfast in our dedication to safeguarding your Veeam backup data.