Object First Appliance Security Assessment

Object First

March 18, 2026

Version 1.2

© 2026 – Prepared by NCC Group Security Services, Inc. for Object First. Portions of this document and the templates used in its production are the property of NCC Group and cannot be copied (in full or in part) without NCC Group's permission.

While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group's services does not guarantee the security of a system, or that computer intrusions will not occur.

Prepared for:
Object First

Prepared by:
William Enright
Timur Duehr
Rob Russell

1 Executive Summary

Synopsis

In the fall of 2025, Object First retained NCC Group to perform a security assessment of its physical appliance server (Release 1.7). The Object First Appliance is an immutable backup solution designed to store backups from other systems in a write-once, non-overwritable format. Object First's objective for this engagement was to identify cybersecurity vulnerabilities that would create unacceptable risks to Object First, and to verify that stored data cannot be modified without proper authorization. NCC Group's assessment encompassed 43 person-days of effort.

Scope

NCC Group's evaluation included:

- **Management Console UI**: Web based administrative console to setup buckets, configure policies, and generally manage the device on a day-to-day basis.
- **Management Web API**: Externally facing web API that can be used to manage the device.
- **Object First Appliance Server**: On-premise solution that enables companies to retain immutable backups of storage buckets.
- **S3 API**: Front-facing API used by Veeam and other systems to create buckets and store objects.
- **Honeypot**: The Honeypot feature deploys a decoy system used to detect cyberattacks.
- **Code Review**: Source code was provided by Object First to support evaluation of each element.

Note that attack vectors requiring physical access to the device, such as access to the Intelligent Platform Management Interface (IPMI), were considered out-of-scope for this assessment.

Key Findings

The assessment uncovered a set of common application flaws, all of which were rated Low or Informational severity. The most notable findings were:

- Weak hashing algorithms were in use in potentially sensitive contexts.
- Various web requests made by the application had SSL/TLS certificate verification explicitly disabled.
- The management application lacks a mechanism to enforce MFA across all users.

All findings were reported to Object First at the end of the engagement.

Positive Findings

Overall Security Improvement: The Object First Appliance has demonstrated notable security improvements since NCC Group's last assessment of the product in Fall 2024. Previously identified vulnerabilities in the areas of authentication, authorization, data validation, and data exposure have been remediated, and no similar vulnerable patterns were observed in the application during this assessment. Only Low and Informational findings were identified during this iteration, mostly involving code security improvement opportunities and minor misconfigurations.

Immutability Controls: All sensitive functionality within the management interface requires admin re-authentication. Actions related to data management, such as deleting S3 buckets, are properly restricted to prevent any deletion of stored data.

New Functionality: Features implemented since the prior engagement conducted in Fall 2024, including Simple Network Management Protocol (SNMP) metrics and Honeypot functionality, were found to implement recognized cybersecurity practices that mitigated unauthorized access, code injection, data exposure, and other potential vulnerabilities.

Appliance Hardening:

- Various hardening steps had been applied to the underlying Ubuntu image in order to improve its security posture.
- Attempts to break out of the restricted CLI and obtain a full shell were unsuccessful.

Honeypot:

- The Honeypot feature successfully identified malicious activity, such as port scanning, and created corresponding alerts within the application UI.
- No misconfigurations were identified related to the Linux services in use by the feature.
- No vulnerabilities were identified within the web UI used to configure the feature.

2 Dashboard

Target Data

Name	Object First Appliance Server (Release 1.7)
Type	Product Security Assessment
Platforms	Linux, AWS, C#, C++, Python
Environment	Testing

Engagement Data

Type	Product Security Assessment
Method	Code-assisted penetration testing
Dates	2025-09-22 to 2025-11-05
Consultants	3
Level of Effort	43 consultant days

Targets

S3 / STS API	Web services API to create buckets and store objects, issue and manage storage API credentials, and manage storage API permissions.
Management User Interface	Primary web application UI for managing an Object First Appliance cluster once it is deployed.
Management API	Web services API used by the web application UI to communicate with and control the Object First Appliance cluster.
Object First Appliance Ubuntu Image	The OS image deployed on the Object First Appliance.

Finding Breakdown

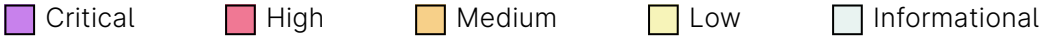
Critical issues	0
High issues	0
Medium issues	0
Low issues	3
Informational issues	4
Total issues	**7**

Category Breakdown

Authentication	1
Cryptography	4
Security Improvement Opportunity	2

Component Breakdown

Host Build Review	1	
Source Code Review	5	
Web Application	1	



3 Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors.

Host Build Review

Title	Status	ID	Risk
Development Utilities Present within Appliance OS	Reported	WP7	Info

Source Code Review

Title	Status	ID	Risk
Weak Cryptographic Hashing Algorithms in Use	Reported	3PW	Low
SSL/TLS Certificate Verification Disabled for Certain Cluster Management APIs	Reported	37G	Low
Insecure Random Number Generation for License Signatures	Reported	7Y3	Info
Potential Cryptographic Padding Oracle within Encryption Utilities	Reported	LTD	Info
Unsafe C/C++ String and Memory Operations	Reported	KLJ	Info

Web Application

Title	Status	ID	Risk
Application Does Not Allow Multi-Factor Authentication Enforcement for All Users	Reported	CD4	Low

4 Finding Field Definitions

The following sections describe the risk rating and category assigned to issues NCC Group identified.

Risk Scale

NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. The risk rating is NCC Group's recommended prioritization for addressing findings. Every organization has a different risk sensitivity, so to some extent these recommendations are more relative than absolute guidelines.

Overall Risk

Overall risk reflects NCC Group's estimation of the risk that a finding poses to the target system or systems. It takes into account the impact of the finding, the difficulty of exploitation, and any other relevant factors.

Rating	Description
Critical	Implies an immediate, easily accessible threat of total compromise.
High	Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.
Medium	A difficult to exploit threat of large-scale breach, or easy compromise of a small portion of the application.
Low	Implies a relatively minor threat to the application.
Informational	No immediate threat to the application. May provide suggestions for application improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.

Impact

Impact reflects the effects that successful exploitation has upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

Rating	Description
High	Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.
Medium	Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.
Low	Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.

Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

Rating	Description
High	Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.
Medium	Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.
Low	Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

Category

NCC Group categorizes findings based on the security area to which those findings belong. This can help organizations identify gaps in secure development, deployment, patching, etc.

Category Name	Description
Access Controls	Related to authorization of users, and assessment of rights.
Auditing and Logging	Related to auditing of actions, or logging of problems.
Authentication	Related to the identification of users.
Configuration	Related to security configurations of servers, devices, or software.
Cryptography	Related to mathematical protections for data.
Data Exposure	Related to unintended exposure of sensitive information.
Data Validation	Related to improper reliance on the structure or values of data.
Denial of Service	Related to causing system failure.
Error Reporting	Related to the reporting of error conditions in a secure fashion.
Patching	Related to keeping software up to date.
Session Management	Related to the identification of authenticated users.
Timing	Related to race conditions, locking, or order of operations.