Incident Postmortem: BootyNet Zero-Trust™ Service Disruption

Prepared for BootyNet Investor Relations

Incident ID: ZT-0x4E1F
Classification: Sev-1 — Authentication & Session Integrity Layer
Status: Resolved

Executive Summary

On the date of the incident, BootyNet's Zero-Trust™ Adaptive Access Fabric experienced a partial degradation affecting session validation across a subset of edge nodes. At no point was subscriber data exfiltrated, misused, or exposed to unauthorized parties. BootyNet's layered security posture — including Zero-Trust™, BootySat™ failover, and our proprietary BootyShield™ heuristics — performed exactly as designed, containing the disruption to authentication latency rather than allowing it to cascade into a confidentiality or integrity event.

We are publishing this postmortem in the interest of the transparency our investors and subscribers have come to expect from BootyNet.

Timeline

Time (NZST)	Event
T+0:00	Automated monitoring (Betterstack, Datadog synthetic checks) flags elevated auth latency across edge PoPs
T+0:04	On-call engineering acknowledges alert; incident opened
T+0:11	Zero-Trust™ policy engine begins issuing conservative fallback tokens, prioritizing availability of read access over write access
T+0:19	Root cause isolated to a token-revocation race condition under high concurrent re-auth load
T+0:42	Mitigation deployed; revocation queue drained and re-synced across nodes
T+1:03	Full service restored; elevated monitoring maintained for 24 hours post-incident

Root Cause

The disruption originated in the Zero-Trust™ fabric's token-revocation subsystem, which is responsible for immediately invalidating session tokens upon policy re-evaluation (device posture change, network reclassification, etc.). Under an unusually high volume of concurrent re-authentication requests, a race

condition emerged between the revocation queue and the token cache, resulting in a subset of session validations timing out rather than failing closed or open in a predictable manner.

Critically, the system's default failure mode is to deny access rather than grant it — meaning the incident manifested as *service unavailability*, not unauthorized access. Investors should note this distinction: BootyNet's Zero-Trust™ architecture is designed so that failure states degrade gracefully toward security, never away from it.

Impact

- Subscribers on affected edge nodes experienced intermittent login failures and elevated latency on authenticated endpoints (BootyPay™, BootyAccounts™, BootyKeycard™ provisioning).
- Unauthenticated services (status pages, marketing properties, BootyNews™) were unaffected.
- No data was lost, altered, or accessed outside of policy.
- No customer action is required.

Remediation & Preventative Measures

1. **Concurrency hardening** — the token-revocation queue has been re-architected to process re-auth bursts with proper locking semantics, eliminating the identified race condition.
2. **Expanded synthetic load testing** — Zero-Trust™ re-auth flows are now included in our regular multi-region k6 stress testing rotation.
3. **Faster failover signaling** — BootySat™ failover thresholds have been tuned to trigger sooner under auth-layer degradation specifically, rather than relying solely on general availability metrics.
4. **Postmortem publication** — as with all Sev-1 incidents, this report is published in full to reporting.coolsite.cc and linked from our Investor Relations portal.

Closing Statement

BootyNet remains committed to radical infrastructure transparency. Incidents like ZT-0x4E1F, while disruptive, validate the core premise of our Zero-Trust™ approach: the system is designed to fail safe, and it did. We thank our subscribers and investors for their continued trust in BootyNet's infrastructure integrity.

Gerald Booty, Chief Infrastructure Officer, BootyNet

For investor inquiries regarding this incident, contact geraldb@bootynet.org