

Finding and fixing known weaknesses

Owner	Tomas Achebe
Proposed by	Tomas Achebe (reviewer), 15 Sep 2026, 14:02 UTC
Approved by	Priya Venkataram (administrator), 15 Sep 2026, 14:28 UTC
Automatic check	Passed: the rule checks and the AI review found no issue

Servers, containers, laptops and product dependencies are scanned every week. Critical weaknesses are fixed within seven days and high ones within thirty. Anything overdue is reported to the VP Engineering each week. Scope: production, staging and the laptop fleet. Cadence: weekly scan, weekly overdue report. Evidence: scan reports and the ticket for each finding.

Requirements met

NIST CSF: ID.RA-01
SOC 2: CC7.1

Risks treated

[BM-RSK-02](#) Ransomware on a laptop or server

Evidence

[BM-EV-004](#) Weekly vulnerability scan, 28 Sep 2026: 6 critical findings open, 3 of them past

Control tests

[BM-TST-06](#) Control test of BM-CTL-06 Finding and fixing known weaknesses (fail)

Audit findings

[BM-AF-01](#) Finding on BM-CTL-06 Finding and fixing known weaknesses

Log entry 95 of Verification/events.jsonl
Entry hash (SHA-256) a1d082da5d396269374fa2099859c64e47470a212d3d9198db79874920bef7da