Incident Overview and Assessment

Incident Overview

Incident ID
INC-2024-0458

Date & Time
2024-06-18, 15:45 UTC

Reported By
John Doe, IT Security

Affected System(s)
Internal File Server (FS-01)

Severity Level
High

Summary
At approximately 15:30 UTC, abnormal network activity was detected on the internal file server (FS-01). Files with confidential data were accessed by an unauthorized user account, and several files were copied to an external location.

Assessment

Root Cause
Compromised user credentials allowed unauthorized access. The userâ€™s workstation was found to be infected by malware.

Scope of Impact
Unauthorized data access could involve personal and sensitive business information. Preliminary review suggests no alteration or deletion of data at this time.

Immediate Actions Taken

- Affected accounts disabled and forced password reset
- Network access for FS-01 limited to critical personnel
- Forensic analysis of logs initiated

Recommended Next Steps

- Full malware scan of connected workstations
- Continued monitoring for anomalous activity
- Review and update access controls

Important Notes

- Use clear, concise language to summarize facts and findings.
- Separate objective observations from analysis and recommendations.
- Specify timelines, affected systems, and containment measures.
- Include actionable next steps for mitigation and prevention.
- Maintain confidentiality when sharing sensitive incident details.