

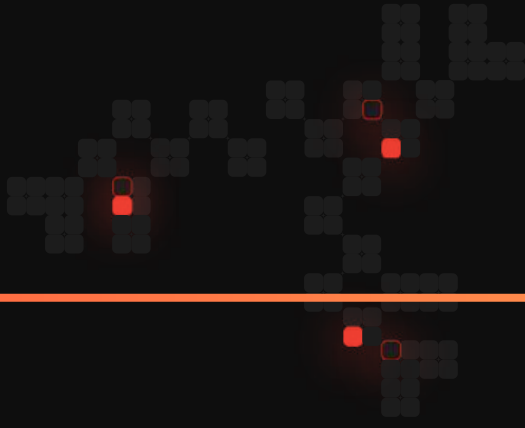


CASE **STUDY**

**SECURED AN EXPOSED SVN
WC.DB FILE IN A MULTINATIONAL
HOLDING COMPANY**



CONTENTS



Overview		3
Ultra-Heals Platform Capabilities		3
Background		4
Incident Discovery		4
Immediate Actions Taken		5
Root Cause Analysis		6
Long-Term Preventive Measures		6
Conclusion		7

Overview

In early 2024, Ultra-Heals, a next-generation AI-powered security platform, identified a significant security vulnerability within a multinational holding company (referred to as "Global Holdings" for confidentiality). This vulnerability involved the public exposure of a Subversion (SVN) wc.db file on the internet, posing severe risks to the company's intellectual property and operational integrity.

Ultra-Heals Platform Capabilities

Ultra-Heals leverages advanced AI to provide comprehensive security platform, including:

- External Attack Surface Management (EASM)
- Digital Risk Protection (DRP)
- Brand Threat Intelligence
- Cloud Security Posture Management (CSPM)
- Compliance Automation

Background

Global Holdings operates in multiple countries across various industries, including technology, finance, and manufacturing. The company uses SVN for version control across its numerous software development projects. The wc.db file, a critical component of SVN's working copy, contains metadata about the repository, including URLs, commit history, and user information.

Incident Discovery

During a routine scan using its EASM module, Ultra-Heals detected that the wc.db file from Global Holdings' SVN repository was accessible on the public internet. This exposure presented several risks:

Repository Information Leakage: Potential unauthorized access to repository metadata.

User Information Exposure: Risk of user credential harvesting and targeted phishing attacks.

Commit History Access: Potential exposure of sensitive code changes and company secrets.

Immediate Actions Taken

Upon detection, Ultra-Heals promptly alerted Global Holdings' security team. The following immediate actions were undertaken:

- **Access Removal:** Public access to the wc.db file was swiftly revoked by reconfiguring web server permissions.
- **Incident Audit:** A comprehensive audit was conducted to determine the extent of the exposure and to check for any unauthorized access attempts.
- **Credential Management:** All potentially exposed credentials were reset, and multi-factor authentication (MFA) was enforced for additional security.
- **Enhanced Monitoring:** Advanced monitoring was deployed to detect any further unauthorized access attempts or anomalies.

Root Cause Analysis

The exposure was attributed to a misconfigured web server during a routine maintenance update. Incorrect permissions had inadvertently made the SVN directory accessible to the public internet.

Long-Term Preventive Measures

To mitigate the risk of future incidents, Global Holdings, with assistance from Ultra-Heals, implemented several long-term measures:

- **Server Configuration Hardening:** Web server configurations were reviewed and strengthened to ensure sensitive files are not publicly accessible.
- **Regular Security Audits:** Scheduled regular security audits using Ultra-Heals' comprehensive scanning and monitoring tools to identify and rectify potential vulnerabilities.
- **Employee Training:** Conducted training sessions for employees on best practices for version control and data security.
- **Ignore Files Implementation:** Ensured that sensitive files are included in .svnignore to prevent accidental commits.
- **Compliance and CSPM:** Leveraged Ultra-Heals' CSPM and compliance automation to ensure all cloud and on-premise infrastructure complies with industry standards and regulations.

- **Backup and Disaster Recovery:** Strengthened backup and disaster recovery plans to mitigate the impact of potential breaches.

Conclusion

The identification and mitigation of the unauthorized phpMyAdmin panel by Ultra-Heals highlight the importance of robust security practices and continuous monitoring. The swift response and comprehensive measures taken by Global Holdings, guided by Ultra-Heals' advanced security platform, successfully mitigated the immediate threat and significantly enhanced the company's overall security posture.

This case study underscores the critical role of AI-powered security solutions like Ultra-Heals in protecting sensitive information and ensuring the security and compliance of multinational enterprises in a complex and ever-evolving threat landscape. The proactive approach taken by Ultra-Heals and Global Holdings serves as a model for addressing and mitigating similar security vulnerabilities in the future.

**To get the free security assessment:
<https://cyberheals.com/free-pentest>**