

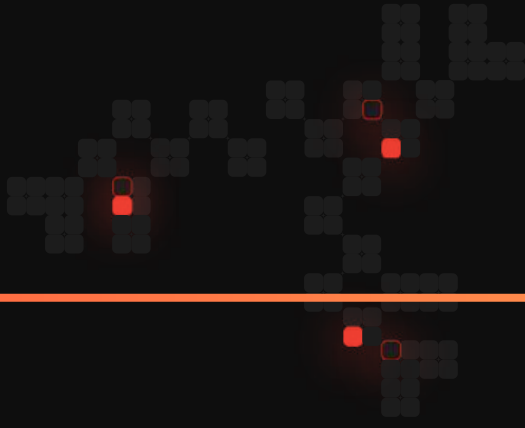


CASE **STUDY**

**IDENTIFIED MICROSOFT
SHAREPOINT AUTHENTICATION
BYPASS VULNERABILITY (CVE-
2023-29357) IN A MULTINATIONAL
HOLDING COMPANY**



CONTENTS



Overview		3
Ultra-Heals Platform Capabilities		3
Background		4
Incident Discovery		4
Risks Associated		5
Immediate Actions Taken		5
Root Cause Analysis		6
Long-Term Preventive Measures		6
Conclusion		8

Overview

Ultra-Heals, a next-generation AI-powered security platform, identified a critical vulnerability within the same multinational holding company (referred to as "Global Holdings" for confidentiality). The vulnerability, CVE-2023-29357, related to Microsoft SharePoint, allowed for authentication bypass, posing a significant risk to the company's data security and integrity.

Ultra-Heals Platform Capabilities

Ultra-Heals offers a comprehensive suite of security services, 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 utilizes Microsoft SharePoint for collaboration and document management. SharePoint's role in storing and managing critical business documents makes it a prime target for security vulnerabilities.

Incident Discovery

During a routine vulnerability assessment using its EASM module, Ultra-Heals detected that Global Holdings' SharePoint installation was susceptible to CVE-2023-29357. This critical vulnerability allowed attackers to bypass authentication mechanisms, potentially leading to unauthorized access to sensitive documents and information.

Risks Associated

- **Unauthorized Data Access:** Potential unauthorized access to sensitive and confidential documents.
- **Data Manipulation and Theft:** Risk of data manipulation, deletion, or exfiltration.
- **Intellectual Property Theft:** Exposure of proprietary information and trade secrets.

Immediate Actions Taken

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

Access Restriction: Temporary measures were implemented to restrict access to the affected SharePoint instance, minimizing potential exploitation.

Patch Deployment: The latest security patch from Microsoft addressing CVE-2023-29357 was promptly applied to mitigate the vulnerability.

Security Audit: A thorough audit was conducted to determine if the vulnerability had been exploited and to assess the extent of potential unauthorized access.

- **Credential Rotation:** Administrative and user credentials were reset to mitigate the risk of any compromised credentials being used maliciously.
- **Enhanced Monitoring:** Real-time monitoring was deployed to detect any future unauthorized access attempts or anomalies.

Root Cause Analysis

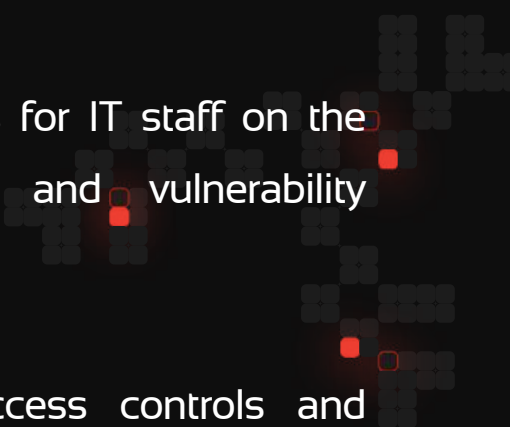
The vulnerability was due to an unpatched SharePoint server. Despite regular updates, the specific patch for CVE-2023-29357 had not been applied due to an oversight in the update management process.

Long-Term Preventive Measures

To prevent future incidents, Global Holdings, with assistance from Ultra-Heals, implemented several long-term measures:

Patch Management Process: Strengthened the patch management process to ensure timely application of all critical updates and patches.

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 IT staff on the importance of timely patch management and vulnerability assessments.

Access Controls: Reviewed and tightened access controls and authentication mechanisms for all critical systems, including SharePoint.

Compliance and CSPM: Leveraged Ultra-Heals' CSPM and compliance automation to ensure all systems comply with industry standards and regulations.

Incident Response Plan: Enhanced the incident response plan to ensure quick and effective response to future vulnerabilities and security incidents.

Conclusion

The identification and mitigation of the exposed wc.db file by Ultra-Heals underscore 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 highlights 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.

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