



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**SQL Injection Vulnerabilities in ManageEngine Products**

Tracking #:432316477

Date:06-11-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity SQL injection vulnerabilities have been discovered and patched in various ManageEngine products, including ADAudit Plus, Exchange Reporter Plus, and ADManager Plus.

## TECHNICAL DETAILS:

Multiple high-severity SQL injection vulnerabilities have been discovered and patched in various ManageEngine products, including ADAudit Plus, Exchange Reporter Plus, and ADManager Plus. These vulnerabilities could allow authenticated attackers to execute arbitrary SQL queries, potentially leading to unauthorized access to sensitive data or system compromise.

### Affected Products and Vulnerabilities:

1. **ADAudit Plus**
  - CVE-2024-5608 and CVE-2024-36485
  - Severity: High
  - Affected versions: All builds below 8121
  - Fixed version: Build 8121
2. **Exchange Reporter Plus**
  - CVE-2024-9459
  - Severity: High
  - Affected versions: Build 5718 and below
  - Fixed version: Build 5719
3. **ADManager Plus**
  - CVE-2024-48878
  - Severity: High
  - Affected versions: 7241 and older
  - Fixed version: 7250

## RECOMMENDATIONS:

- **Immediate Patching:** Update all affected ManageEngine products to their respective fixed versions as soon as possible.
- **Access Review:** Conduct a thorough review of user access to these applications, ensuring that only necessary personnel have authenticated access.
- **Network Segmentation:** Implement or review network segmentation to limit the potential impact of a successful exploitation.
- **Monitoring:** Enhance monitoring for suspicious activities, particularly focusing on database queries and access patterns in the affected products.
- **Incident Response:** Update incident response plans to include specific steps for addressing potential SQL injection attacks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.



## REFERENCES:

- <https://www.manageengine.com/products/exchange-reports/advisory/CVE-2024-9459.html>
- <https://www.manageengine.com/products/ad-manager/admanager-kb/cve-2024-48878.html>
- <https://www.manageengine.com/products/active-directory-audit/cve-2024-5608.html>
- <https://www.manageengine.com/products/active-directory-audit/cve-2024-36485.html>