

**Notification Date:** October 31, 2025

## SECURITY ADVISORY

# Multiple Vulnerabilities in Advantech WebAccess/VPN (Versions $\leq$ 1.1.4)

### Summary

Multiple vulnerabilities were identified in **Advantech WebAccess/VPN 1.1.4 and earlier**, including stored cross-site scripting, SQL injection, directory traversal, and command injection flaws. These issues could allow authenticated or low-privileged users to execute arbitrary scripts, access or modify sensitive data, and in some cases, inject commands or disclose system information. Users are recommended to upgrade to WebAccess/VPN 1.1.5.

### Issue Description

- 1. NetworksController.addNetworkAction() – Stored Cross-Site Scripting**  
*Severity:* Score 8.1 (High), CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34236
- 2. StandaloneVpnClientsController.addStandaloneVpnClientAction() – Stored Cross-Site Scripting**  
*Severity:* Score 7.3 (High), CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34237
- 3. AjaxStandaloneVpnClientsController.ajaxDownloadRoadWarriorConfigFileAction() – Absolute Directory Traversal to Information Disclosure**  
*Severity:* Score 4.9 (Medium), CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34238
- 4. AppManagementController.appUpgradeAction() – Command Injection**  
*Severity:* Score 7.2 (High), CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34239
- 5. AjaxDeviceController.ajaxActionValidateTable() – SQL Injection**  
*Severity:* Score 8.1 (High), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34240

6. **AjaxDeviceController.ajaxDeviceAction() – SQL Injection**  
*Severity:* Score 5.4 (Medium), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34241
7. **AjaxNetworkController.ajaxAction() – SQL Injection**  
*Severity:* Score 8.1 (High), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34242
8. **AjaxFwRulesController.ajaxNetworkFwRulesAction() – SQL Injection**  
*Severity:* Score 5.4 (Medium), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34243
9. **AjaxFwRulesController.ajaxDeviceFwRulesAction() – SQL Injection**  
*Severity:* Score 5.4 (Medium), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34244
10. **AjaxStandaloneVpnClientsController.ajaxAction() – SQL Injection**  
*Severity:* Score 5.4 (Medium), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34245
11. **AjaxPrevalidationController.ajaxAction() – SQL Injection**  
*Severity:* Score 5.4 (Medium), CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34246
12. **NetworksController.addNetworkAction() – SQL Injection**  
*Severity:* Score 3.8 (Low), CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N  
*Affected products:* WebAccess/VPN 1.1.4 and prior  
*Also known as:* CVE-2025-34247

## Solution

Users are recommended to upgrade to WebAccess/VPN 1.1.5.

## Acknowledgement

These vulnerabilities have been discovered by Alex Williams from Pelleria Technologies.

## Revision History

2025-10-31 Advisory published