CYBER ADVISORY

Thursday, July 02, 2026 **CAL-CSIC-202607-A-001**

Trio of Vulnerabilities Impacting IBM Websphere Application Server Help System

Cross-Site Scripting	Path Traversal	Potential for Pivoting	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a trio of vulnerabilities impacting IBM WebSphere Application Server's built-in Integrated Help System and its General Administrative Console Help System. CVE-2026-11708 and CVE-2026-11712 are critically rated vulnerabilities that both carry a CVSS 3.1 score of 9.3[1] [2], while CVE-2026-11595 is a medium-rated vulnerability that carries a CVSS 3.1 score of 4.3.[3]

CVE-2026-11708 is a cross-site scripting vulnerability that impacts the administrative console's *integrated* help system in IBM's WebSphere Application Server. The vulnerability allows an attacker who can invoke the console's help functions to inject arbitrary malicious HTML or JavaScript that can run with the privileges of the authenticated console session. Successful exploitation allows the attacker to capture sensitive data, hijack admin sessions, and allow further pivoting within the targeted server.[4]

CVE-2026-11712 is another cross-site scripting vulnerability that impacts the general administrative console help system in IBM's WebSphere Application Server. The vulnerability allows an attacker to inject and execute malicious arbitrary client-side scripts in a user's browser when viewing the help pages. Successful exploitation allows the attacker to steal session cookies, mimic as legitimate users, and redirect users to malicious sites. The attacker would be able to compromise the confidentiality, availability of the administrative interface.[5]

CVE-2026-11595 is a path traversal vulnerability that impacts the general administrative console help system in IBM's WebSphere Application Server. The vulnerability allows the attacker to construct URLs that reference directories outside the intended file space. Successful exploitation gives the attacker access to configuration data, log files, and sensitive artifacts that the web application server processes that could be used to further perpetuate internal pivoting on the targeted server.[6]

IBM has acknowledged these vulnerabilities and has published a security advisory with interim fixed software releases with post-installation instructions for affected server versions. There are no workarounds for these vulnerabilities. There is no Proof-of-Concept for these vulnerabilities, nor is there evidence of them being exploited in the wild or as a zero-day.

The Cal-CSIC recommends following IBM's remediation guidance as soon as possible. For additional details for all three vulnerabilities, please use this link:

IBM Security Bulletin: https://www.ibm.com/support/pages/security-bulletin-ibm-websphere-application-server-affected-multiple-vulnerabilities-cve-2026-11712-cve-2026-11595-cve-2026-11708

IBM Remediation Guidance: https://www.ibm.com/support/pages/node/7278563

Affected Products and Versions

Product	Affected Software Version	Interim Release/Permanent Fix Status
IBM WebSphere Application Integrated Help System	9.0, 8.5	Interim Fix: PH71756 Applied Fix Pack (Target Availability 3Q2026)
IBM WebSphere Application Help System	9.0, 8.5	Interim Fix: PH71756 Applied Fix Pack (Target Availability 3Q2026)

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] OpenCVE; "CVE-2026-11708"; https://app.opencve.io/cve/CVE-2026-11708; accessed 02 July 2026
[2] OpenCVE; "CVE-2026-11712"; https://app.opencve.io/cve/CVE-2026-11712; accessed 02 July 2026
[3] OpenCVE; "CVE-2026-11595"; https://app.opencve.io/cve/CVE-2026-11595; accessed 02 July 2026
[4] IBM Support; "Security Bulletin: IBM WebSphere Application Server is affected by multiple vulnerabilities (CVE-2026-11712, CVE-2026-11595, CVE-2026-11708)"; https://www.ibm.com/support/pages/security-bulletin-ibm-websphere-application-server-affected-multiple-vulnerabilities-cve-2026-11712-cve-2026-11595-cve-2026-11708; accessed 02 July 2026
[5] IBM Support; "Security Bulletin: IBM WebSphere Application Server is affected by multiple vulnerabilities (CVE-2026-11712, CVE-2026-11595, CVE-2026-11708)"; https://www.ibm.com/support/pages/security-bulletin-ibm-websphere-application-server-affected-multiple-vulnerabilities-cve-2026-11712-cve-2026-11595-cve-2026-11708; accessed 02 July 2026
[6] IBM Support; "Security Bulletin: IBM WebSphere Application Server is affected by multiple vulnerabilities (CVE-2026-11712, CVE-2026-11595, CVE-2026-11708)"; https://www.ibm.com/support/pages/security-bulletin-ibm-websphere-application-server-affected-multiple-vulnerabilities-cve-2026-11712-cve-2026-11595-cve-2026-11708; accessed 02 July 2026