Security Bulletin: IBM i is affected by a privilege escalation vulnerability in Web Administration GUI [CVE-2026-2311]

Security Bulletin

Summary

Web Administration GUI for IBM i is vulnerable to privilege escalation caused by an invalid authorization check as described in the vulnerability details section.

Vulnerability Details

CVEID: CVE-2026-2311 *(https://www.cve.org/CVERecord?id=CVE-2026-2311)*

DESCRIPTION: IBM i is vulnerable to privilege escalation caused by an invalid IBM i Web Administration GUI authorization check. A malicious actor could cause user-controlled code to run with administrator privilege.

CWE: CWE-284: Improper Access Control *(https://cwe.mitre.org/data/definitions/284.html)*

CVSS Source: IBM

CVSS Base score: 6.4

CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Affected Product Version(s)	Affected Product Feature(s) or License Program Product(s)
IBM i	7.6	5770DG1
IBM i	7.5	5770DG1
IBM i	7.4	5770DG1
IBM i	7.3	5770DG1
IBM i	7.2	5770DG1

Remediation/Fixes

IBM strongly recommends addressing the vulnerability now.

IBM i Release	5770-DG1 PTF Number(s)	PTF Download Link(s)
7.6	SJ08417	https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08417 *(https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08417)*
7.5	SJ08418	https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08418 *(https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08418)*
7.4	SJ08419	https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08419 *(https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08419)*
7.3	SJ08604	https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08604 *(https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08604)*

IBM i Release	5770-DG1 PTF Number(s)	PTF Download Link(s)
7.2	SJ08818	https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08818 *(https://www.ibm.com/mysupport/s/fix-information?legacy=SJ08818)*

IBM recommends users running unsupported versions of affected products upgrade to a supported and fixed version of affected products.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

Subscribe to My Notifications *(https://www.ibm.com/support/pages/node/718119)* to be notified of important product support alerts like this.

References

Complete CVSS v3 Guide

On-line Calculator v3

Related Information

IBM Secure Engineering Web Portal *(http://www.ibm.com/security/secure-engineering/bulletins.html)*

IBM Product Security Incident Response Blog *(http://www.ibm.com/blogs/psirt)*

Acknowledgement

Change History

15 Apr 2026: Initial Publication

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced

product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Cross-reference information

Product	Component	Platform	Version
IBM i		IBM i	7.6.0, 7.5.0, 7.4.0, 7.3.0, 7.2.0
IBM i 7.2 Preventative Service Planning		IBM i	7.2.0
IBM i 7.3 Preventative Service Planning		IBM i	7.3.0
IBM i 7.4 Preventative Service Planning		IBM i	7.4.0
IBM i 7.5 Preventative Service Planning		IBM i	7.5.0
IBM i 7.6 Preventative Service Planning		IBM i	7.6.0

Document Information

More support for:

IBM i *(https://www.ibm.com/mysupport/s/topic/0TO50000000QW2ZGAW)*

Software version:

7.6.0, 7.5.0, 7.4.0, 7.3.0, 7.2.0

Operating system(s):

IBM i

Document number:

7269560

Modified date:

15 April 2026

Initial Publish date:

15 April 2026