



High

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Security Guardium Database Activity Monitor	10.0	All	All	All
Application	ibm	Security Guardium Database Activity Monitor	10.01	All	All	All
Application	ibm	Security Guardium Database Activity Monitor	10.1	All	All	All
Application	ibm	Security Guardium Database Activity Monitor	8.2	All	All	All
Application	ibm	Security Guardium Database Activity Monitor	9.0	All	All	All
Application	ibm	Security Guardium Database Activity Monitor	9.1	All	All	All
Application	ibm	Security Guardium Database Activity Monitor	9.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

IBM Security Guardium Database Activity Monitor CVE-2016-0241 Local Security Bypass Vulnerability

IBM Security Bulletin: IBM Security Guardium Database Activity Monitor is affected by Improper Authentication Vulnerability (CVE-2016-0241)

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[591177](#) Moxa AWK-3131A Web Application onekey Information Disclosure Vulnerability (TALOS-2016-0241)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)