



Kados R10 GreenBee SQL Injection via user2reset

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-25694 |
| State | PUBLISHED |
| Assigner | VulnCheck |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-05 21:16:48 UTC |
| Updated | 2026-04-07 19:19:02 UTC |
| Description | Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database |

Risk And Classification

Primary CVSS: v4.0 8.8 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000650000 probability, percentile 0.201260000 (date 2026-04-06)

Problem Types: CWE-89 | CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------|-----------|-------|----------|--|
| 4.0 | disclosure@vulncheck.com | Secondary | 8.8 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/S |
| 4.0 | CNA | CVSS | 8.8 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/S |
| 3.1 | nvd@nist.gov | Primary | 9.1 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N |
| 3.1 | disclosure@vulncheck.com | Secondary | 8.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N |
| 3.1 | CNA | CVSS | 8.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------|---------|--------------|--------|---------|----------|
| Application | Marmotech | Kados | r10_greenbee | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|-----------------------|------------------------------------|-----------------------|---------------|
| CNA | Kados | Kados R10 GreenBee | affected R10 GreenBee | Not specified |

References

| Reference | Source | Link | Tags |
|--|--|--|-------|
| www.exploit-db.com/exploits/46505 | disclosure@vulncheck.com | www.exploit-db.com | Explo |
| www.vulncheck.com/advisories/kados-r10-greenbee-sql-injection-via-user2reset | disclosure@vulncheck.com | www.vulncheck.com | Third |
| www.kados.info | disclosure@vulncheck.com | www.kados.info | Produ |
| sourceforge.net/projects/kados | disclosure@vulncheck.com | sourceforge.net | Produ |
| CVE Program record | CVE.ORG | www.cve.org | canor |
| NVD vulnerability detail | NVD | nvd.nist.gov | canor |

Vendor Comments And Credit

Discovery Credit

CNA: Mehmet EMIROGLU (en)

There are currently no legacy QID mappings associated with this CVE.

© [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