



CVE-2017-3564

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3564
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-24 19:59:04 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: RBAC). The supported version is 11.4.4.0.0. The vulnerability allows a user to execute arbitrary code on the target system. The vulnerability is due to a buffer overflow in the Solaris component. An attacker who exploited this vulnerability could cause the target system to crash or execute arbitrary code. Oracle has released a patch for this vulnerability. Users are advised to apply the patch as soon as possible.

Risk And Classification

Primary CVSS: v3.0 8.2 HIGH from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | Easily "exploitable" vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Solaris.

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.2	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.9		AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Oracle	Solaris	11.3	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	Solaris Operating System	affected 11.3	Not specified

References

Reference

Oracle Critical Patch Update - April 2017

Solaris Flaws Let Remote and Local Users Obtain Elevated Privileges and Deny Service and Let Local Users Access and Modify Data - Secur

Oracle Solaris CVE-2017-3564 Local Security Vulnerability

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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](#)