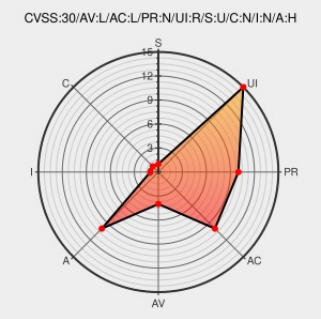
CVE-2018-1000524

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1000524

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Minisphere from Spheredev contain the following vulnerability:

miniSphere version 5.2.9 and earlier contains a Integer Overflow vulnerability in layer_resize() function in map_engine.c that can result in remote denial of service. This attack appear to be exploitable via the victim must load a specially-crafted map which calls SetLayerSize in its entry script. This vulnerability appears to have been fixed in 5.0.3, 5.1.5, 5.2.10 and later.

CVE-2018-1000524 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix integer overflow in layer_resize in map_engine.c by	Third Party Advisory github.com	MISC github.com/fatcerberus/minisphere/pull/268

xiaoyinl · Pull Request #268 · fatcerberus/miniSphere · GitHub	text/html	
Fix integer overflow in layer_resize in map_engine.c (#268) · fatcerberus/miniSphere@252c1ca · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/fatcerberus/minisphere/commit/252c1ca184cb38e1acb917aa0e451c5f0

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spheredev	Minisphere	All	All	All	All

cpe:2.3:a:spheredev:minisphere:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→