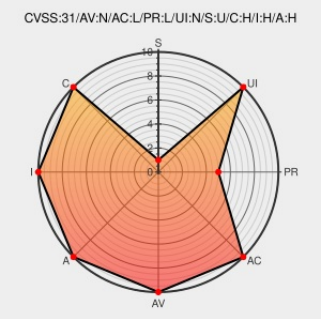
CVE-2019-10808

Published on: 03/11/2020 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:58:00 PM UTC

CVE-2019-10808

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



Certain versions of Utilitify from Xcritical.software contain the following vulnerability:

utilitify prior to 1.0.3 allows modification of object properties. The merge method could be tricked into adding or modifying properties of the Object.prototype.

CVE-2019-10808 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Broken Link github.com text/plain Inactive Link Not Archived	MISC github.com/xcritical-software/utilitify/commit/88d6e27009823338bf319ffb768fe6b08e8ad2d1,

Prototype Pollution in utilitify | Snyk	Exploit Patch Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-UTILITIFY-559497

Related QID Numbers

981936 Nodejs (npm) Security Update for utilitify (GHSA-9534-h433-2rjf)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xcritical.software	Utilitify	All	All	All	All
Application	Xcritical.software	Utilitify	All	All	All	All

cpe:2.3:a:xcritical.software:utilitify:*:*:*:*:*:node.js:*:*

cpe:2.3:a:xcritical.software:utilitify:*:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→