# CVE Detail – CVE-2018-3721

lodash node module before 4.17.5 suffers from a Modification of Assumed-Immutable Data (MAID) vulnerability via defaultsDeep, merge, and mergeWith functions, which allows a malicious user to modify the prototype of "Object" via \_\_proto\_\_, causing the addition or modification of an existing property that will exist on all objects.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.40863

## CVSS Scoring

CVSS v3.1 Score: 6.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
* CWE-471: Modification of Assumed-Immutable Data (MAID)

## CAPEC(s)

* CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs
* CAPEC-180: Exploiting Incorrectly Configured Access Control Security Levels
* CAPEC-384: Application API Message Manipulation via Man-in-the-Middle
* CAPEC-385: Transaction or Event Tampering via Application API Manipulation
* CAPEC-386: Application API Navigation Remapping
* CAPEC-387: Navigation Remapping To Propagate Malicious Content
* CAPEC-388: Application API Button Hijacking
* CAPEC-77: Manipulating User-Controlled Variables

## ATT&CK Techniques

* T1574.010: Services File Permissions Weakness

## Used By (Actors/Tools)

* BlackEnergy (malware)

## Affected Products

* cpe:2.3:a:lodash:lodash:\*:\*:\*:\*:\*:node.js:\*:\*
* cpe:2.3:a:netapp:active\_iq\_unified\_manager:-:\*:\*:\*:\*:linux:\*:\*
* cpe:2.3:a:netapp:active\_iq\_unified\_manager:-:\*:\*:\*:\*:vmware\_vsphere:\*:\*
* cpe:2.3:a:netapp:active\_iq\_unified\_manager:-:\*:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:netapp:system\_manager:9.0:\*:\*:\*:\*:\*:\*:\*