



CVE-2018-15691

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

Summary

CVE	CVE-2018-15691
State	PUBLIC
Assigner	vuln@ca.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-30 14:29:00 UTC
Updated	2021-04-12 14:17:00 UTC
Description	Insecure deserialization of a specially crafted serialized object, in CA Release Automation 6.5 and earlier, allows attackers to

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Release Automation	All	All	All	All
Application	Ca	Release Automation	All	All	All	All
Application	Ca	Release Automation	All	All	All	All

References

Reference	Source
CA Release Automation Object Deserialization Error Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SE
CA20180829-03: Security Notice for CA Release Automation	CC
CA Release Automation NiMi 6.5 - Remote Command Execution - Java remote Exploit	E>
CA Release Automation CVE-2018-15691 Arbitrary Code Execution Vulnerability	BI
CVE Program record	CV
NVD vulnerability detail	NV

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)