



CVE-2019-18956

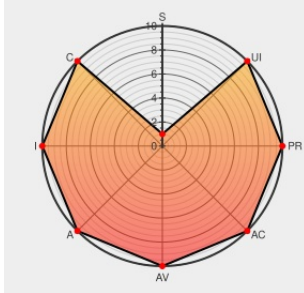
Published on: 12/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:07 PM UTC

CVE-2019-18956

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Dv2eemvc](#) from [Divisait](#) contain the following vulnerability:

Divisa Proxia Suite 9 < 9.12.16, 9.11.19, 9.10.26, 9.9.8, 9.8.43 and 9.7.10, 10.0 < 10.0.32, and 10.1 < 10.1.5, SparkSpace 1.0 < 1.0.30, 1.1 < 1.1.2, and 1.2 < 1.2.4, and Proxia PHR 1.0 < 1.0.30 and 1.1 < 1.1.2 allows remote code execution via untrusted Java deserialization.

The proxia-error cookie is insecurely deserialized in every request (GET or POST). Thus, an unauthenticated attacker can easily craft a serial1.0lized payload in order to execute arbitrary code via the prepareError function in the com.divisait.dv2ee.controller.MVCCControllerServlet class of the dv2eemvc.jar component. allows remote code execution via untrusted Java deserialization. The proxia-error cookie is insecurely deserialized in every request (GET or POST). Thus, an unauthenticated attacker can easily craft a serialized payload in order to execute arbitrary code via the prepareError function in the com.divisait.dv2ee.controller.MVCCControllerServlet class of the dv2eemvc.jar component. Affected products include Proxia Premium Edition 2017 and Sparkspace.

CVE-2019-18956 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact

PARTIAL

Impact

PARTIAL

Impact

PARTIAL

CVE References

Description	Tags	Link
advisories/2019/CVE-2019-18956 at master · blackarrowsec/advisories · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/blackarrowsec/advisories/tree/master/2019/CVE-2019-18956

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Divisait	Dv2eemvc	All	All	All	All
Application	Divisait	Dv2eemvc	All	All	All	All
Application	Divisait	Dv2eemvc	All	All	All	All
Application	Divisait	Proxia Phr	All	All	All	All
Application	Divisait	Proxia Phr	All	All	All	All
Application	Divisait	Proxia Suite	All	All	All	All
Application	Divisait	Proxia Suite	All	All	All	All
Application	Divisait	Sparkspace	All	All	All	All
Application	Divisait	Sparkspace	All	All	All	All

cpe:2.3:a:divisait:dv2eemvc:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:dv2eemvc:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:dv2eemvc:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:proxia_phr:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:proxia_phr:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:proxia_suite:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:proxia_suite:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:sparkspace:*.*.*.*.*.*.*:

cpe:2.3:a:divisait:sparkspace:*.*.*.*.*.*.*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)