```
arraynetworks ag1500 -
arraynetworks ag1500 -
arraynetworks ag1500fips -
arraynetworks vxag -
arraynetworks ag1500v5 -
arraynetworks ag1000 -
arraynetworks ag1000 -
arraynetworks ag100v5 -
arraynetworks ag120v5 -
arraynetworks ag1500 -
arraynetworks ag150 -
arraynetworks ag150 -
arraynetworks arrayos ag *

Description:

Array Networks Array AG Series and vxAG (9.4.0.481 and earlier) allow
remote code execution. An attacker can browse the filesystem on
the SSL VPN gateway using a flags attribute in an HTTP header
without authentication. The product could then be exploited
```

through a vulnerable URL. The 2023-03-09 vendor advisory stated "a new Array AG release with the fix will be available soon."

Main problems:

Components:

CVE-2023-28461 - Score: 9.8

0 0

287 no CWE Description available