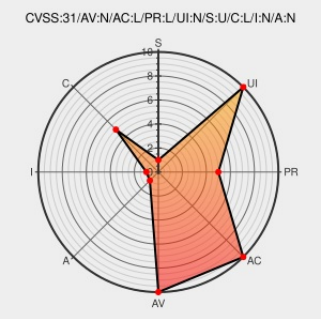
CVE-2018-13374

Published on: 01/22/2019 12:00:00 AM UTC

Last Modified on: 06/03/2021 11:15:00 AM UTC

CVE-2018-13374

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



Certain versions of Fortios from Fortinet contain the following vulnerability:

A Improper Access Control in Fortinet FortiOS 6.0.2, 5.6.7 and before, FortiADC 6.1.0, 6.0.0 to 6.0.1, 5.4.0 to 5.4.4 allows attacker to obtain the LDAP server login credentials configured in FortiGate via pointing a LDAP server connectivity test request to a rogue LDAP server instead of the configured one.

CVE-2018-13374 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS, fortiADC** version **FortiOS 6.0.2, 5.6.7 and before, FortiADC 6.1.0, 6.0.0 to 6.0.1, 5.4.0 to 5.4.4**

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: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

Read-only admins can obtain LDAP credentials configured in FortiGate using LDAP test connectivity feature | FortiGuard	Vendor Advisory fortiguard.com text/html	CONFIRM fortiguard.com/advisory/FG-IR-18-157
FortiGate FortiOS < 6.0.3 - LDAP Credential Disclosure - Hardware webapps Exploit	Exploit Third Party Advisory www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 46171

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CswWorks	The #Conti group is associated with 3 vulnerabilities CVE-2020-0796, CVE-2018-13374, CVE-2018-13379. If these were… twitter.com/i/web/status/1…	2021-07-07 12:22:43
@CswWorks	We analyzed three CVEs being exploited by the Conti group - CVE-2020-0796, CVE-2018-13374, CVE-2018-13379, and here… twitter.com/i/web/status/1…	2021-09-08 11:30:15

← Previous ID

Next ID→