



CVE-2018-8753

Published on: 08/15/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:41 PM UTC

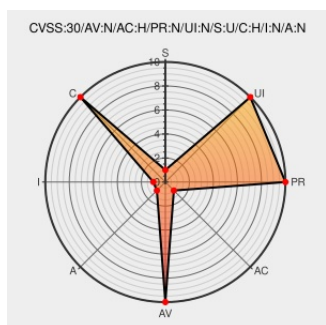
CVE-2018-8753

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Cos Core** from **Clavister** contain the following vulnerability:

The IKEv1 implementation in Clavister cOS Core before 11.00.11, 11.20.xx before 11.20.06, and 12.00.xx before 12.00.09 allows remote attackers to decrypt RSA-encrypted nonces by leveraging a Bleichenbacher attack.

CVE-2018-8753 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Practical Bleichenbacher Attacks on IPsec IKE	Third Party Advisory web-in-security.blogspot.com text/html	e MISC web-in-security.blogspot.com/2018/08/practical-bleichenbacher-attacks-on-ipsec-ike.html
CLAV-SA-0157 - Bleichenbacher Oracle Vulnerability	Vendor Advisory	CONFIRM

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	Clavister	Cos Core	All	All	All	All
Application	Clavister	Cos Core	All	All	All	All
cpe:2.3:a:clavister:cos_core:*****:						
cpe:2.3:a:clavister:cos_core:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)