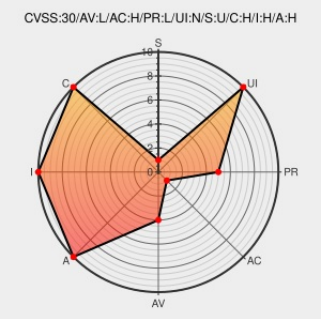
CVE-2018-18466

Published on: 03/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

CVE-2018-18466

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



Certain versions of Securaccess from Securenvoy contain the following vulnerability:

** DISPUTED ** An issue was discovered in SecurEnvoy SecurAccess 9.3.502. When put in Debug mode and used for RDP connections, the application stores the emergency credentials in cleartext in the logs (present in the DEBUG folder) that can be accessed by anyone. NOTE: The vendor disputes this as a vulnerability since the disclosure of a local account password (actually an alpha numeric passcode) is achievable only when a custom registry key is added to the windows registry. This action requires administrator access and the registry key is only provided by support staff at securenvoy to troubleshoot customer issues.

CVE-2018-18466 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
CVE-2018-18466 - Excellium Services	Third Party Advisory www.excellium-services.com text/html	MISC www.excellium-services.com/cert-xlm-advisory/cve-2018-18466/

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	Securenvoy	Securaccess	9.3.502	All	All	All
Application	Securenvoy	Securaccess	9.3.502	All	All	All

cpe:2.3:a:securenvoy:securaccess:9.3.502:*:*:*:*:*:*:*:

cpe:2.3:a:securenvoy:securaccess:9.3.502:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→