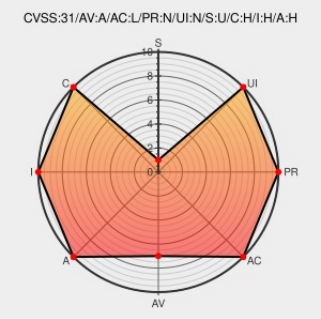
CVE-2018-5354

Published on: 09/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-5354

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



Certain versions of Password Reset Client from Anixis contain the following vulnerability:

The custom GINA/CP module in ANIXIS Password Reset Client before version 3.22 allows remote attackers to execute code and escalate privileges via spoofing. When the client is configured to use HTTP, it does not authenticate the intended server before opening a browser window. An unauthenticated attacker capable of conducting a spoofing attack can redirect the browser to gain execution in the context of the WinLogon.exe process. If Network Level Authentication is not enforced, the vulnerability can be exploited via RDP.

CVE-2018-5354 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
GitHub - missing0x00/CVE-2018-5354: CVE-2018-5354	Exploit	MISC github.com/missing0x00/CVE-2018-5354

GitHub - missingOx00/CVE-2018-5354: CVE-2018-5354	Exploit Third Party Advisory github.com text/html	MISC github.com/missingOx00/CVE-2018-5354
Password policy and password reset software	Vendor Advisory anixis.com text/html	MISC anixis.com

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

Exploit/POC from Github

CVE-2018-5354

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Anixis	Password Reset Client	All	All	All	All
Application	Anixis	Password Reset Client	All	All	All	All

cpe:2.3:a:anixis:password_reset_client:*:*:*:*:*:*:*:*:

cpe:2.3:a:anixis:password_reset_client:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→