Microsoft Entra Connect Health flaw exposed tenant metadata to attackers



Microsoft told affected customers that attackers used a flaw in the Entra Connect Health API to read tenant metadata, including technical contact emails. No passwords or tokens were exposed; phishing is the main risk.

- The flaw was introduced on July 23, 2026 and went undetected until November 9.
- Microsoft deployed a service-side fix on November 19 and concluded its investigation the next day.
- Exposed data included technical contact emails, tenant ID and name, license tier and sync status; passwords, hashes, tokens and keys were not exposed.
- Microsoft found no unauthorized configuration changes, and no customer update is required.
- The number of affected tenants and the identity of the attackers have not been disclosed.

Microsoft has notified organizations that attackers exploited a vulnerability in the Microsoft Entra Connect Health API to read tenant-level metadata. Connect Health is a cloud monitoring service that gives administrators a view of the health and alerts of their on-premises identity infrastructure.

What happened

According to the notification, the flaw was introduced on July 23, 2026 and was not detected until November 9. Microsoft applied a service-side fix on November 19 and finished its investigation the following day, confirming unauthorized read-only access to metadata. It found no unauthorized configuration changes.

The responses the intruders reached contained technical contact email addresses, tenant ID, display name, initial domain, country code, region scope, license tier, directory synchronization status, last sync timestamp and onboarding status. Passwords, hashes, tokens, valid cryptographic keys, on-premises server and Active Directory topology, and Azure subscription information were not exposed. Microsoft has not said how many tenants were affected or who was responsible.

Why it matters

No remediation is needed from customers for the flaw itself, but the exposed email addresses and tenant facts make targeted phishing more convincing, particularly messages that mention Entra or Connect Health. Risk is higher if a technical contact also holds a privileged role such as Global Administrator.

Microsoft also advises verifying the notification by signing in to the Azure portal directly and checking the Security Advisory in Azure Service Health, rather than following links in an email.

What to do now

1. Alert the SOC, IT operations and tenant technical contacts to watch for phishing that references the organization, Entra or Connect Health.
2. Verify any Microsoft notification by signing in to the Azure portal directly and checking Azure Service Health, not through email links.
3. Require phishing-resistant MFA and Privileged Identity Management just-in-time activation for technical contacts who hold privileged roles.
4. Run Microsoft's read-only PowerShell script to see what the API could return for your tenant, noting values may have changed since exposure.
5. Review Entra audit and sign-in logs and Azure Activity Logs for unexpected Connect Health changes or unusual administrative activity.