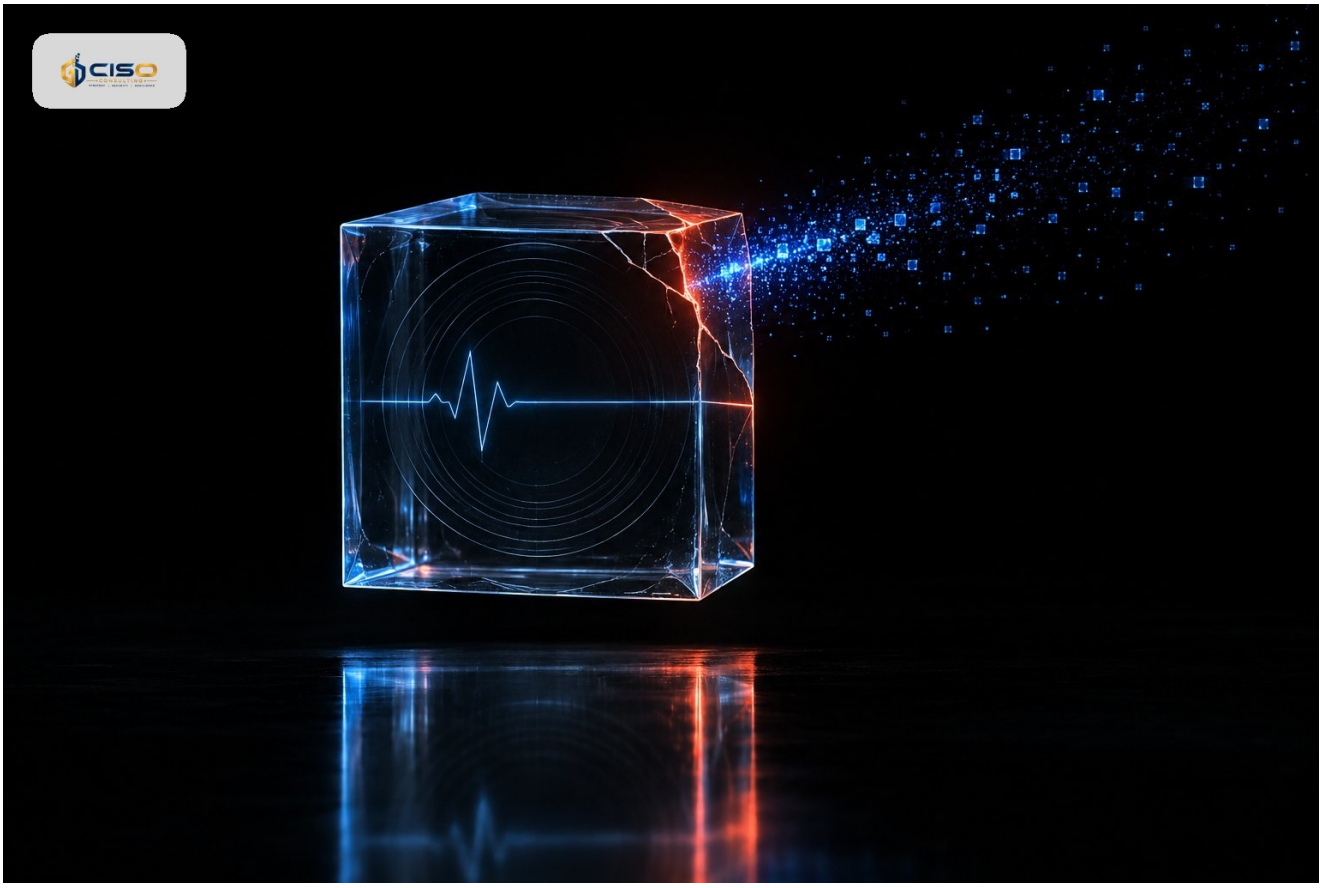
Reported exploitation of a Microsoft Entra Connect Health flaw to steal tenant data



BleepingComputer reports that a flaw in Microsoft Entra Connect Health has been exploited to steal tenant data. The source text was unreadable beyond the headline, so details remain unconfirmed.

- The reported issue affects Microsoft Entra Connect Health.
- The flaw is reported as exploited, not merely theoretical.
- The reported impact is theft of tenant data.
- Technical details, affected versions and fixes could not be confirmed from the source text.

What has been reported

BleepingComputer published a report under the headline that a flaw in **Microsoft Entra Connect Health** was exploited to steal tenant data. The headline is the only part of the source we could read, so we do not state how the attack works, who is behind it, who was affected or whether a patch exists.

What we cannot confirm

We have no confirmed information on a CVE identifier, affected versions, the type of data taken, the number of victims or Microsoft's response. We will not speculate on these points. Institutions should treat this as an early signal and read Microsoft's own guidance and the original article before drawing conclusions.

Recommended approach

Organisations that synchronise on-premises directories with Microsoft Entra ID, or that use Entra Connect Health for monitoring, should check whether the service is deployed in their environment. They should confirm who administers it and review recent activity around it. A calm, evidence-based review is more useful than urgent changes made without detail. Update this assessment once Microsoft or the original reporter publishes technical specifics, and record the review in your risk register as part of normal third-party and cloud service oversight.

What to do now

1. Check whether Entra Connect Health or Entra Connect is deployed and identify its owner.
2. Read Microsoft's official advisory and the original article for affected versions and fixes.
3. Review sign-in and administrative activity in Entra ID for unusual events.
4. Review privileged roles and service accounts linked to directory synchronisation.
5. Record the issue in the risk register and brief the CISO until details are confirmed.