Xen Orchestra authentication bypass flaw under active exploitation



Vates VMS warns that a critical authentication bypass in Xen Orchestra, tracked as VSA-2026-062, is being exploited in the wild. It has no CVE identifier yet.

- Vates VMS, a French software company, issued the alert for Xen Orchestra.
- The flaw is an authentication bypass tracked as VSA-2026-062.
- The vendor says it is being actively exploited in the wild.
- No CVE identifier has been assigned yet.
- The issue lies in how REST cookie parsing handles the authentication token.

Vates VMS has warned that a critical vulnerability in Xen Orchestra, its virtualization management platform, is

being actively exploited. The flaw is an authentication bypass tracked as VSA-2026-062 and does not yet have a CVE identifier.

What the vendor describes

According to the vendor's alert, the problem sits in the REST interface. A specially formed authentication token in a cookie is parsed into an empty object, and the REST authentication logic then passes that object onward. The source excerpt is cut off at this point, so the full mechanism and the exact consequences are not covered here. The headline indicates that attackers are using the flaw to gain administrative access.

Why it matters

A management platform for virtual infrastructure holds broad control over the workloads it administers. Administrative access obtained without valid credentials is therefore a serious exposure, and active exploitation means that waiting is not a safe option. Because no CVE exists yet, tools that depend on CVE feeds may not flag the issue, so teams should track the vendor advisory directly.

The source does not state which versions are affected or whether a patch is available. Teams should consult the Vates VMS advisory for those details before acting.

What to do now

1. Identify every Xen Orchestra instance in your estate, including test and forgotten deployments.
2. Read the Vates VMS advisory VSA-2026-062 and apply the vendor's fix or mitigation as soon as it is confirmed.
3. Restrict access to the Xen Orchestra REST interface to trusted management networks until remediation is complete.
4. Review authentication and administrative activity logs for unexpected admin sessions or changes.
5. Track VSA-2026-062 manually in your vulnerability register, since no CVE exists yet.