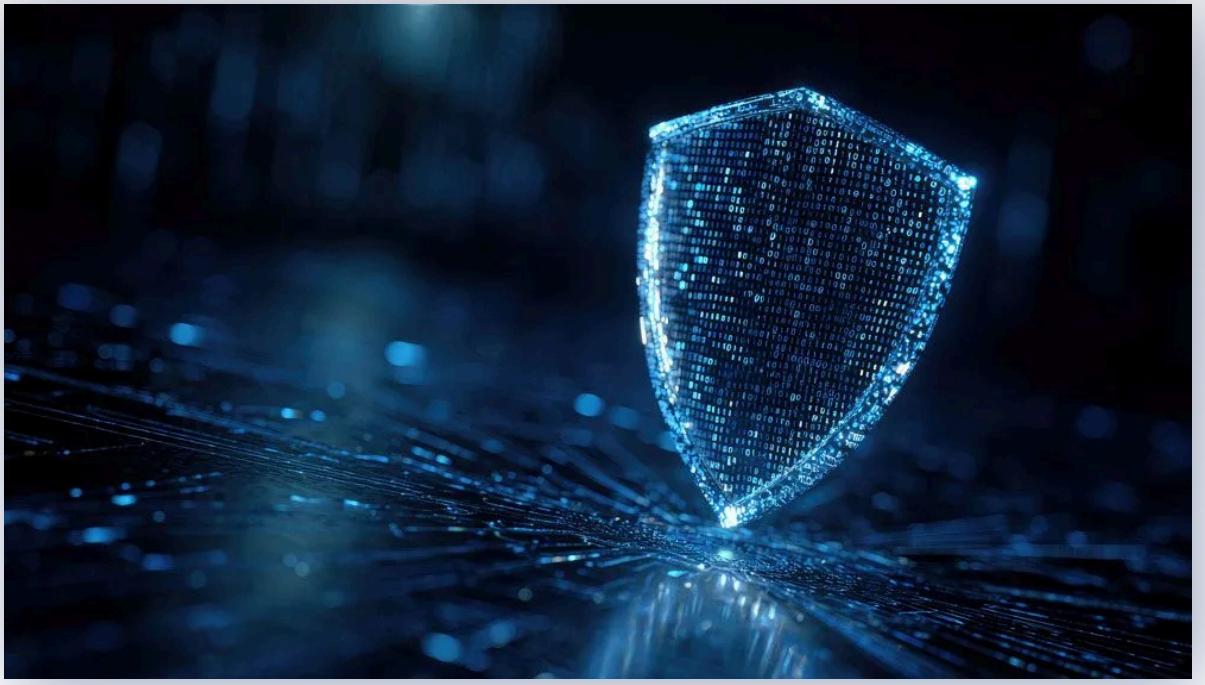
Breaking Down the Advantech WISE-DeviceOn CVE-2025-34256 Vulnerability



April 15, 2026
Cybersecurity

By: Alex Williams

Unlocking the full potential of IoT requires more than powerful hardware—it demands strong security. Advantech, a global leader in industrial computing and IoT solutions with $2 billion in annual revenue, powers industries like smart manufacturing and healthcare IT through advanced industrial PCs, embedded systems, and edge computing platforms. Organizations rely on Advantech WISE-DeviceOn, an Internet of Things (IoT) management platform that enables seamless monitoring of Windows and Ubuntu agents through a web application.

DeviceOn's Authentication System

WISE-DeviceOn uses JSON Web Tokens (JWT) for its authorization system. JWTs are an authorization and information exchange system that can be used as an alternative to standard cookies. JWTs use the following format:

eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.

eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlf(

dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk

JWTs consists of three sections separated by periods: header, payload, and signature. Each section is Base64-encoded. The previous JWT can be decoded into the following:

```
{
  "typ": "JWT",
  "alg": "HS256"
}
{
  "iss": "joe",
  "exp": 1300819380,
  "http://example.com/is_root": true
}
{
    // Signature
}
```

Follow Us

Recent Posts

Unleashing the Power of a 3D Data Security Architecture

Identity Is the New Perimeter: The 5 Must Haves for Securing AI Access Control

Visit Blog