Siemens Desigo CC and Gridscale X affected by critical Node.js Brotli flaw (CVE-2026-111497)



CISA reports that Siemens Desigo CC V8 and V9 and two Gridscale X products are affected by CVE-2026-111497, a critical Node.js Brotli flaw (CVSS 9.8). Siemens has released fixed versions and advises updating.

- CVE-2026-111497, nicknamed 'Node2Shell', is an out-of-bounds write in the Brotli decoder bundled with Node.js, rated CVSS v3 9.8.
- It could let a remote attacker corrupt memory and potentially run arbitrary code.
- Affected: all Desigo CC V8 and V9 versions, Gridscale X DSA 5.3 up to below 5.4, and Gridscale X PSS® E below 36.8.0.
- Node.js released security updates on October 21, 2026; Siemens has issued new versions of the affected products.

> - Sectors listed include critical manufacturing, energy and information technology.

CISA has published an advisory on the impact of a critical Node.js vulnerability on several Siemens products. The flaw, tracked as **CVE-2026-111497** and referred to as "Node2Shell", sits in the Brotli decoder bundled with Node.js.

What is affected

The issue is an out-of-bounds write that could allow a remote attacker to cause memory corruption and potentially execute arbitrary code. It carries a CVSS v3 score of 9.8. Node.js released security updates on October 21, 2026.

The affected Siemens products are:

- Desigo CC family V8, all versions
- Desigo CC family V9, all versions
- Gridscale X DSA, versions from 5.3 up to but not including 5.4
- Gridscale X PSS® E, versions below 36.8.0

The advisory lists critical manufacturing, energy and information technology among the relevant sectors.

What to do

Siemens has released new versions of the affected products and recommends updating to the latest versions. Institutions running Desigo CC for building management or Gridscale X in energy-related work should confirm whether their deployments fall within the listed ranges and plan the update through normal change control. The source does not describe active exploitation, so treat this as a priority patching task rather than an emergency, while recognising the high severity score.

What to do now

1. Inventory all Desigo CC V8/V9 and Gridscale X DSA and PSS® E instances, including those in OT or building-management networks.
2. Check installed versions against the affected ranges and apply the Siemens updates to the latest versions.
3. Until patched, limit network exposure of affected systems to trusted segments and users.
4. Record the exposure and remediation in vulnerability management and OT risk registers.
5. Ask vendors and integrators whether other software in your estate bundles Node.js and is affected.