

Specimen — illustrative example

Solstice Grid Services is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Produced by RiskWoven.com. Produced by fixed rules from the information supplied. No AI drafting was involved, so no review stage applied.

Known-exploited vulnerability findings

Solstice Grid Services · Produced by RiskWoven.com

Checked against: CISA Known Exploited Vulnerabilities catalog, retrieved 21 September 2026 · **Assets checked:** 6
· **Assets with findings:** 4 · **Findings:** 8 · **Used in ransomware:** 6

Every finding below is a vulnerability CISA records as actively exploited, in a product you run. Work through them in the order shown. This is not a full vulnerability scan: vulnerabilities outside the catalog are not covered.

CVE-2023-34362: Progress MOVEit Transfer SQL Injection Vulnerability

Actively exploited · Version affected · Used in ransomware

Asset: Progress Software MOVEit Transfer 2023.0.1 · **Asset criticality:** High · **CISA due date:** 23 June 2023

Progress MOVEit Transfer contains a SQL injection vulnerability that could allow an unauthenticated attacker to gain unauthorized access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or delete database elements.

Required action: Apply updates per vendor instructions.

Version 2023.0.1 is inside an affected range in the CVE record.

CVE-2023-22518: Atlassian Confluence Data Center and Server Improper Authorization Vulnerability

Actively exploited Version affected Used in ransomware

Asset: Atlassian Confluence Server 7.19.0 · **Asset criticality:** Not set · **CISA due date:** 28 November 2023

Atlassian Confluence Data Center and Server contain an improper authorization vulnerability that can result in significant data loss when exploited by an unauthenticated attacker. There is no impact on confidentiality since the attacker cannot exfiltrate any data.

Required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Version 7.19.0 is inside an affected range in the CVE record.

CVE-2023-46805: Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability

Actively exploited Version affected Used in ransomware

Asset: Ivanti Connect Secure 22.6R2 · **Asset criticality:** High · **CISA due date:** 22 January 2024

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways contain an authentication bypass vulnerability in the web component that allows an attacker to access restricted resources by bypassing control checks. This vulnerability can be leveraged in conjunction with CVE-2024-21887, a command injection vulnerability.

Required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Version 22.6R2 is inside an affected range in the CVE record.

CVE-2024-21887: Ivanti Connect Secure and Policy Secure Command Injection Vulnerability

Actively exploited Version affected Used in ransomware

Asset: Ivanti Connect Secure 22.6R2 · **Asset criticality:** High · **CISA due date:** 22 January 2024

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contain a command injection vulnerability in the web components of these products, which can allow an authenticated administrator to send crafted requests to execute code on affected appliances. This vulnerability can be leveraged in conjunction with CVE-2023-46805, an authenticated bypass issue.

Required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Version 22.6R2 is inside an affected range in the CVE record.

CVE-2024-21893: Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability

Actively exploited Version affected Used in ransomware

Asset: Ivanti Connect Secure 22.6R2 · **Asset criticality:** High · **CISA due date:** 2 February 2024

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure), Ivanti Policy Secure, and Ivanti Neurons contain a server-side request forgery (SSRF) vulnerability in the SAML component that allows an attacker to access certain restricted resources without authentication.

Required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Version 22.6R2 is inside an affected range in the CVE record.

CVE-2025-22457: Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability

Actively exploited Version affected Used in ransomware

Asset: Ivanti Connect Secure 22.6R2 · **Asset criticality:** High · **CISA due date:** 11 April 2025

Ivanti Connect Secure, Policy Secure, and ZTA Gateways contains a stack-based buffer overflow vulnerability that allows a remote unauthenticated attacker to achieve remote code execution.

Required action: Apply mitigations as set forth in the CISA instructions linked below.

Version 22.6R2 is not among the fixed releases the CVE record lists.

CVE-2022-26138: Atlassian Questions For Confluence App Hard-coded Credentials Vulnerability

Actively exploited**Version not confirmed**

Asset: Atlassian Confluence Server 7.19.0 · **Asset criticality:** Not set · **CISA due date:** 19 August 2022

Atlassian Questions For Confluence App has hard-coded credentials, exposing the username and password in plaintext. A remote unauthenticated attacker can use these credentials to log into Confluence and access all content accessible to users in the confluence-users group.

Required action: Apply updates per vendor instructions.

The CVE record does not list affected versions under this product's name, so the version was not checked.

CVE-2024-38475: Apache HTTP Server Improper Escaping of Output Vulnerability

Actively exploited**Version affected**

Asset: Apache HTTP Server 2.4.54 · **Asset criticality:** Medium · **CISA due date:** 22 May 2025

Apache HTTP Server contains an improper escaping of output vulnerability in mod_rewrite that allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

Required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Version 2.4.54 is inside an affected range in the CVE record.