

2025 年 9 月 29 日

DCSpider ご契約者各位

株式会社テラスカイ
製品事業ユニット サービスエンジニアリング本部

DCSpider に含まれる XML 外部実体参照 (XXE) 脆弱性に関するお知らせ

平素は格別のご高配を賜り厚く御礼申し上げます。

DCSpider にて、一部のクライアントアプリケーションに XML 外部実体参照に関する脆弱性 (CWE-611) があることが判明しました。

下記内容をご確認の上、ご対応をお願いいたします。

記

1. 影響を受ける製品及びバージョン

DCSpider 全バージョン

2. 影響範囲

- ・ クライアントアプリケーション
 - － DCSpider Studio for Web
 - － CLI Console
 - － ScriptRunner
 - － ScriptRunnerProxy
 - － WebConsole

3. 脆弱性による影響

影響範囲に記載しているクライアントアプリケーションにおいて、攻撃者によって通信を改ざんされることにより、サーバアプリケーションがインストールされたファイルシステムにある情報を不正に読み取られたり、サービス運用妨害 (DoS) 状態を引き起こされる可能性があります。

4. お客様へのお願い事項

本脆弱性につきましては、影響範囲に記載のクライアントアプリケーションと DCSpider Server 間の通信が外部ネットワークを経由しない場合、影響を受けることはございません。

また、外部ネットワークを経由する場合であっても、HTTPS による暗号化通信をご設定いただいている環境では影響を受けません。

設定方法の詳細につきましては「Studio ヘルプ > サービスガイド > サービスの運用 > 詳細なトピック > HTTPS サーバ設定」をご参照ください。

お手数をおかけいたしますが、貴社のご利用環境をご確認のうえ、影響を受けることのないようご対応くださいますようお願い申し上げます。

なお、ご確認方法や対応方法についてご不明な点がございましたら、サポートセンターまでお問い合わせください。

5. お問い合わせ先

ご不明点などございましたら、以下のサポートセンターよりお問い合わせください。

<https://d.terrasky.jp/ProductSupport>

以上