ソフトウェアセキュリティ管理

1 脆弱性開示ポリシー

双一力（寧波）有限公司は、製品のメーカーとして、自社製品とサービス業務のセキュリティに極めて関心を持ち、プライバシーとデータセキュリティの重要性を認識しています。各種セキュリティ対策における脆弱性の対応は、企業セキュリティの向上と切り離せない関係にあり、関係各方が共同で取り組む必要があります。もしあなたが、当社製品の使用時に潜在的なセキュリティ上の脆弱性を発見した、または発見したと信じている場合は、できるだけ早くその発見内容を当社に開示することを奨励いたします。詳細は、本脆弱性開示ポリシーに従います。当社は、各報告者から報告された問題に対して、専門の担当者が対応し、分析し、処理する体制を整えており、迅速な返信をいたします。

2 脆弱性のフィードバックと処理プロセス

2.1 脆弱性のフィードバック

双一力では、すべてのユーザーの安全な体験を最優先に保障しています。当社製品の使用中に潜在的なセキュリティ上の脆弱性や問題に遭遇した場合は、すぐに当社に通報することを奨励いたします。皆様の積極的なご参加こそ、製品のセキュリティ向上に欠かせない

重要な要素です。

報告手順:

1. 問題特定：セキュリティ問題または特定した脆弱性について、詳細に記載してください。その際、問題のある製品型番と具体的な状況を明記してください。

2. 添付情報：可能であれば、問題再現の手順、影響範囲、関連するスクリーンショットやログを提供してください。

3. 報告内容の提出：製品セキュリティチームに対し、メール marketing@risen.com 宛てに問題を報告してください。

2.2 脆弱性処理フロー

ステップ 1：報告者は脆弱性の詳細情報を提供する必要があります。

ステップ 2：双一力は受け取った脆弱性情報をチェックし、検証し、評価を行います。

ステップ 3：脆弱性を修正し、製品の修正状況を検証します。

ステップ 4：新バージョンの製品をリリースし、更新を可能にします。

ステップ 5：報告者に対して処理結果を返信します。

ステップ 6：更新後、製品の安定性をモニタリングします。

2.3 脆弱性審査段階

1. 当該報告は受け取り後 3 営業日以内に確認され、初歩的な報告が提出されて評価が行

われます。

2. 内部評価は 7 営業日以内に完了し、脆弱性の修正が完了するか、修正計画が策定されます。

2.4 脆弱性修正と完了段階

1. 重大な脆弱性は完了後 3 営業日以内に修正評価が行われます。

2. 高リスクの脆弱性は完了後 7 営業日以内に修正評価が行われます。

3. 中程度リスクの脆弱性は完了後 30 営業日以内に修正評価が行われます。

4. 低リスクの脆弱性は完了後 60 営業日以内に修正評価が行われます。

5. 脆弱性が環境やハードウェアの制限によるものであることが確認された場合、最終的な修理時期は実際の状況に応じて決定されます。

6. 深刻な影響や重大な影響に対しては、個別の緊急セキュリティ通告が発表されます。

3 脆弱性評価基準

脆弱性の危害度に応じて、これらのレベルは 4 つの層に分けられます：極端なリスク、高リスク、中程度のリスク、および低リスク。当社は脆弱性報告を受け取ると、ISO/IEC 30111 を参照して内部で解決する一連の措置を講じます。すべての報告された脆弱性は、一般脆弱性評価システム CVSS 3.1 基準に合致するようにスコアリングされます。

3.1 極端な脆弱性

1. リモートで直接システム権限 (サーバー権限、クライアント権限、スマートデバイス) にアクセスできる脆弱性。これには、任意のコード実行、任意のコマンド実行、WebShell のアップロードと使用などが含まれるが、これらに限定されない。

2. この核心業務システムには論理設計上の欠陥が存在し、これには、任意のアカウントのパスワード変更に何らの保護制限がないこと、任意のアカウントでのログインなどが含まれるが、これらに限定されない。

3. これは、ネットワーク情報の漏洩に直結する深刻な脆弱性を持つ業務システムで、これには核心 データベースの SQL インジェクション脆弱性などが含まれるが、これに限定されない。

4. モバイル端末：リモートコード実行の脆弱性で、多数の非インタラクティブユーザー数に直接影 響を与える可能性がある。

5. 装置：インターネット環境において、リモートでデバイスの実行権限（例えば、その他のダウン ロード権限、ユーザーデータの取得、デバイスへのリモートアクセスなど）を取得できる、インタラ クティブなリモートコマンド実行の脆弱性環境が存在する場合。

3.2 高リスク脆弱性

1. この脆弱性は、オンラインサーバー上の機密情報の漏洩に直結し、これには核心システムのソー スコード漏洩、サーバーの機密ログファイルのダウンロードなどが含まれるが、これらに限定されな い。

2. この核心業務システムでは、他人の身元を利用してすべての機能を実行できる脆弱性

や、核心業 務システムにおける重要または機密な無許可行為の脆弱性が存在する。

3. 管理プラットフォームへの無許可アクセスと管理者機能の使用。これには、機密なバックエンド 管理者アカウントのログインが含まれるが、関連プラットフォームの活動、ユーザー層、機能の重要 性、およびユーザー情報の機密性は、高リスク脆弱性の評価基準とみなされる。

4. 高リスクの情報漏洩脆弱性。これには、直接利用可能な機密データの漏洩や、大量のユーザー識 別情報の漏洩につながる利用可能な脆弱性が含まれるが、これらに限定されない。

5. SSRF における応答付き脆弱性で、双一力の内部ネットワークにアクセスできる場合。

6. モバイル端末：複数の範囲でモバイルクライアント機能を使用し、高リスク操作（例えば、ファイルの読み書き、SMS の読み書き、クライアントデータの読み書き）を実行するための第三者アプリ、および高リスクの機密情報漏洩。

7. 装置：近接またはローカルエリアネットワークから装置の実行権限を取得する（例えば、他のユーザーデータのダウンロードや装置へのリモートアクセス)。近接またはローカルエリアネットワーク内における対話型のリモートコマンド実行の脆弱性がない場合。

8. 装置：装置を永久的にサービス拒否状態にする脆弱性。これには、システム装置へのリモートサービス拒否攻撃 (装置が使用不能になり、完全に永久的に損傷する、またはシステム全体を書き換える必要がある）などが含まれるが、これらに限定されない。この攻撃は装置との対話を許さず、迅速な大量複製が可能な攻撃である。

3.3 中リスク脆弱性

1. 一般的な情報漏洩で、これにはモバイルクライアントにおける平文でのパスワード保存、サーバーやデータベースの機密情報を含むソースコード圧縮ファイルのダウンロードなどが含まれるが、これらに限定されない。

2. システムにおける論理設計上の欠陥、例えば温度保護の論理設計における欠陥など。

3. 応答のない SSRF の脆弱性。

4. ユーザー識別情報を取得するために対話が必要な脆弱性で、これには CSRF、保存型 XSS、JSONP による機密情報のハイジャックなどの機密操作に限定されるわけではないが、これらを含む。

5. リモートサービス拒否の脆弱性で、オンラインアプリケーションの特定の機能が無効になる可能性がある（他のユーザーにも影響を与えることを証明する必要がある）。

6. スマートデバイスをサービス拒否状態にする脆弱性。例えば、システムデバイスがローカルから発生する永久的なサービス拒否攻撃 (デバイスが使用不能になり：完全に永久的に損傷するか、また はオペレーティングシステム全体を書き換える必要がある）を被る場合、リモート攻撃（リモートで の一時停止や再起動）による一時的なサービス拒否攻撃を引き起こす脆弱性、そして攻撃が迅速な大 量複製が可能である場合。

7. 一般的な業務システムが、他人の身元を利用してその権限を超えるすべての機能を実行できる状 況。

3.4 低リスク脆弱性

1. これらの脆弱性は、フィッシング攻撃に利用される可能性があり、URL リダイレクトの脆弱性な どが含まれるが、これらに限定されない。

2. 低リスクの論理設計上の欠陥。

3. 二次的な情報漏洩の脆弱性で、パス漏洩、git ファイルの漏洩、サーバー側の業務ログの内容など が含まれるが、これらに限定されない。

4. これらの脆弱性は、フィッシング攻撃やハッキングに利用される可能性があり、任意の URL の 調整や反射型 XSS の脆弱性などが含まれるが、これらに限定されない。

5. モバイル端末：ローカルサービス拒否（第三者コンポーネントの権限以外に起因するサービス拒 否を含むが、これらに限定されない)、軽微な情報漏洩（個々のユーザーのみに影響を及ぼす）など。

6. デバイスを一時的にサービス拒否状態にする脆弱性。これには、ローカル攻撃による一時的なサ ービス拒否攻撃に起因する脆弱性（デバイスを出荷時の設定に戻す必要がある）などが含まれるが、 これらに限定されない。

3.5 無視すべき問題

1. BUG でセキュリティと関係のない問題で、ネットワークのページ開放速度、乱雑な書式などが含 まれるが、これらに限定されない。

2. 提出された報告が極めて簡単で、報告内容に基づいて対応が困難な場合。これには、何度も報告 者とコミュニケーションを取っても再現できない脆弱性などが含まれるが、

これらに限定されない。

3. 利用不能または無害な通報で、悪戯的な CSRF（ユーザーに対するもの)、他人に影響を与えない ローカルサービス拒否、Self - XSS、PDF XSS、非機密情報の漏洩（内部 IP、ドメイン名)、メール ボムなどが含まれるが、これらに限定されない。

4. 実用性のないソースコード漏洩。

5. 当該ハードウェア製品が双一力のモジュールではない場合のセキュリティ問題、またはハードウ ェア自体の欠陥。

6. 双一力が自発的に開示した、または外部から既に開示されているセキュリティ関連の問題。

7. セキュリティ製品、アプリケーション、もしくはもはやメンテナンスされていない WEB アプリ ケーションにおける問題。

8. 双一力が内部で既知であり、すでに修正済みの脆弱性であることを自己検証できる場合。

9. 第三者コンポーネントのライセンスに起因するサービス拒否。

双一力に提供されるすべての製品の脆弱性情報、製品脆弱性報告に含まれるすべての情報を含め、送 信された情報は双一力の所有と使用に供されます。

双一力はいつでも本ポリシーを修正する権利を保有します。