脆弱性対応ポリシー

セキュリティ勧告に従い、「暁星重工業㈱［HYOSUNG HEAVY INDUSTRIES CORPORATION］」は、提供する製品およびサービスにおけるセキュリティ脆弱性に対処するための適切な手順を確立しています。また、公開されている脆弱性データベースを定期的に監視し、ペネトレーションテストを実施しています。
本ページでは、弊社の脆弱性開示方針（脆弱性ディスクロージャーポリシー）の概要について説明します。

脆弱性に関する報告

暁星重工業㈱は、弊社のサービスのセキュリティ強化に貢献していただけるすべての方々からの報告を歓迎いたします。 安全な報告プロセスを確保するため、以下のガイドラインに従って報告書を提出してください。

善意の報告者として、次のガイドラインを遵守していただきますようお願いいたします。
- 脆弱性の実証に必要な最小限の検証のみを行ってください。
  実際のユーザーデータの変更、削除、またはダウンロードは固く禁止されています。
- システムダウンタイム、サービスの低下、または一般ユーザーに影響を与える可能性のあるテストは避けてください。
- 暁星ジャパンによる分析および公式パッチが完了するまで、報告された脆弱性を第三者や公に開示せず、秘密を保持してください。

上記のガイドラインを遵守し、善意で脆弱性を報告していただいた方に対しては、民事上および刑事上の法的措置を講じないことを保証いたします。暁星重工業㈱は、皆様の貴重な努力を尊重し、保護します。

以下の「お問い合わせ」リンクから報告書を提出してください。その際、以下の詳細を含めることを推奨します。
- 報告者の連絡先詳細
- システム仕様（例：製品名、ファームウェアバージョン）
- エラー現象または関連ログ
- 技術的な詳細（例：脆弱性の再現手順、サンプルパケットキャプチャ）

お問い合わせ / Contact Us: https://www.hyosung.co.jp/contact/

対応プロセス

暁星重工業㈱は、受領した脆弱性に迅速かつ透明性をもって対応するため、以下のステップに従って処理を行います。

段階 1. 受領および確認［受領後5営業日以内］
- 報告書が正常に受領されると、担当者が報告者へ確認のメールを送信します。

段階 2. 分析および検証［受領後10営業日以内］
- 社内の専門部署が脆弱性の再現性を検証し、リスクレベル（CVSSメトリクスなどに基づく）を評価した上で、有効な脆弱性であるかどうかを判断します。

段階 3. 修正およびパッチ適用［重要度に応じてスケジュールは異なります］
- 製品開発部署と製品セキュリティチームが連携し、脆弱性パッチの開発および適用を行います。
- ただし、各セキュリティ脆弱性の特性はそれぞれ異なるため、特定の解決スケジュールを保証することはできません。修正対応には、ソフトウェアの修正、新製品バージョンのリリース、またはセキュリティガイドラインの更新などが含まれる場合があります。プロセスの全期間を通じて、パッチが最終確定する前にすべての懸念事項が解決されるよう、脆弱性の発見者および影響を受けるベンダーと継続的に調整を行います。

段階 4. 結果の共有および完了
- 修正が正常に完了した後、その結果を報告者と共有し、公式ウェブサイトに公開します。

最近のセキュリティアップデート

Category	Patch Version	Affected Products	CVE	CVSS	Last Update
ESS	3.04.02 3.03.02 3.02.02 3.01.02	HS-EM4200GLO HS-EM3000GLO HS-EM2625GLO HS-EM1500GLO	CVE-2023-48795	7.5	26.06.05
ESS	3.03.01	HS-EM3000GLO			26.05.15
ESS	3.01.01	HS-EM1500GLO			26.05.15
ESS	3.02.01	HS-EM2625GLO			26.05.06
ESS	3.04.01	HS-EM4200GLO			26.05.06