취약점 공개 정책

보안 권고사항에 따라, 효성중공업(주)은 자사 제품 및 서비스의 보안 취약점을 처리하기 위한 적절한 절차를 수립하고 있습니다.
아울러 당사는 정기적으로 공개 취약점 데이터베이스를 모니터링하고 침투 테스트를 수행합니다.

본 페이지는 당사의 취약점 공개 정책을 요약한 것입니다.

취약점 신고

효성중공업(주)은 당사 서비스의 보안을 강화하는 데 도움을 주시는 모든 제보자 분들의 제보를 환영하며,
안전한 제보를 위해 아래와 같이 제보를 해주시기 바랍니다.

선의의 제보자로서, 아래의 사항을 준수해 주시길 부탁드립니다.
- 취약점 증명을 위해 필요한 최소한의 확인만 해주시기 바랍니다. 실제 사용자 데이터의 수정, 삭제 및 다운로드는 절대 금지됩니다.
- 시스템 가동 중단, 서비스 지연 등 일반 사용자의 서비스 이용에 지장을 주는 테스트는 삼가 주시기 바랍니다.
- 제보하신 취약점은 효성중공업이 분석하고 패치(수정)를 완료할 수 있도록 공식 조치가 끝나기 전까지 대외에 공개하지 말아 주십시오.

위 가이드라인을 준수하여 선의로 취약점을 제보해 주신 제보자 분에 대해서는, 당사는 어떠한 민·형사상 법적 조치도 취하지 않을 것을 약속합니다. 효성중공업(주)은 제보자 분들의 노력을 존중하며 보호하겠습니다.

제보는 아래의 “문의하기“ 링크를 통해 진행하면 되며, 아래 내용이 포함되는 것을 권장합니다.
- 제보자 연락처
- 제품 명, 펌웨어 버전과 같은 시스템 정보
- 문제 상황 또는 관련 로그
- 취약점을 유발하는 단계, 샘플 패킷 캡쳐 등 기술적 세부정보

문의하기 / Contact Us: https://www.hyosung.co.jp/ko/contact/

취약점 관리 프로세스

효성중공업(주)은 접수된 취약점을 아래와 같은 단계에 따라 신속하고 투명하게 처리하고 있습니다.

1. **접수 및 확인** [접수 후 5영업일 이내]
   - 제보가 정상적으로 접수되면, 담당자가 제보자에게 확인 메일을 발송합니다.

2. **분석 및 검증** [접수 후 10영업일 이내]
   - 회사 내 담당부서에서 취약점의 재현 여부를 검증하고, 위험도(CVSS 기준 등)를 평가하여 유효한 취약점인지 판정합니다.

3. **취약점 조치** [심각도에 따라 기간 차등]
   - 제품개발 주관부서와 제품보안 주관부서간 협력하여 취약점 패치(수정)를 진행합니다.
   - 단, 각 보안 취약점 사례는 모두 다르기 때문에 특정 해결 기한을 보장할 수 없습니다.
     해결 조치에는 소프트웨어 수정, 새 제품 버전 출시 및/또는 보안 지침 업데이트가 포함될 수 있습니다 .
     전체 과정 동안 취약점 발견자 및 영향을 받는 공급업체와 지속적으로 협의하여 모든 우려 사항이 해결된 후에야 패치를 완료합니다.

4. **결과 공유 및 완료**
   - 조치가 완료되면 제보자에게 결과를 공유하고 홈페이지에 공개합니다.

최신 보안업데이트 내역

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