{"file_collection_verification_code": "0ef5adab744d6ece874208eb361730d01633847c", "crypto_spec_version": 3.0, "package_name": "22011121", "crypto_evidence": {"cb7ff4ef8b7aa4c702863af823c02a2e9c926df2": {"file_paths": ["D:\\gitProject\\CDBackEnd\\storage\\22011121\\temp.txt"], "hits": [{"matched_text": "SHA256", "line_text": "SHA256", "line_number": 10, "file_index_begin": 107, "file_index_end": 113, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "BIP", "line_text_before_2": "ETH_GETBLOCKBYNUMBER", "line_text_before_3": "ETH_BLOCKNUMBER", "line_text_after_1": "CRC32", "line_text_after_2": "AES", "line_text_after_3": "CIPHER", "evidence_type": "algorithm/hash/SHA2", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "SHA3", "line_text": "SHA3", "line_number": 15, "file_index_begin": 135, "file_index_end": 139, "line_index_begin": 0, "line_index_end": 4, "line_text_before_1": "RSA", "line_text_before_2": "CIPHER", "line_text_before_3": "AES", "line_text_after_1": "HMAC", "line_text_after_2": "SHASUM", "line_text_after_3": "ECDH", "evidence_type": "algorithm/hash/SHA3", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "HMAC", "line_text": "HMAC", "line_number": 16, "file_index_begin": 140, "file_index_end": 144, "line_index_begin": 0, "line_index_end": 4, "line_text_before_1": "SHA3", "line_text_before_2": "RSA", "line_text_before_3": "CIPHER", "line_text_after_1": "SHASUM", "line_text_after_2": "ECDH", "line_text_after_3": "MD5", "evidence_type": "algorithm/hash/HMAC", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "ECDH", "line_text": "ECDH", "line_number": 18, "file_index_begin": 152, "file_index_end": 156, "line_index_begin": 0, "line_index_end": 4, "line_text_before_1": "SHASUM", "line_text_before_2": "HMAC", "line_text_before_3": "SHA3", "line_text_after_1": "MD5", "line_text_after_2": "RIPEMD160", "line_text_after_3": "DIFFIE_HELLMAN", "evidence_type": "algorithm/asymmetric/ECC", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "MD5", "line_text": "MD5", "line_number": 19, "file_index_begin": 157, "file_index_end": 160, "line_index_begin": 0, "line_index_end": 3, "line_text_before_1": "ECDH", "line_text_before_2": "SHASUM", "line_text_before_3": "HMAC", "line_text_after_1": "RIPEMD160", "line_text_after_2": "DIFFIE_HELLMAN", "line_text_after_3": "PBKDF2", "evidence_type": "algorithm/hash/MD5", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "RIPEMD160", "line_text": "RIPEMD160", "line_number": 20, "file_index_begin": 161, "file_index_end": 170, "line_index_begin": 0, "line_index_end": 9, "line_text_before_1": "MD5", "line_text_before_2": "ECDH", "line_text_before_3": "SHASUM", "line_text_after_1": "DIFFIE_HELLMAN", "line_text_after_2": "PBKDF2", "line_text_after_3": "ECDSA", "evidence_type": "algorithm/hash/RIPEMD", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "ECDSA", "line_text": "ECDSA", "line_number": 23, "file_index_begin": 193, "file_index_end": 198, "line_index_begin": 0, "line_index_end": 5, "line_text_before_1": "PBKDF2", "line_text_before_2": "DIFFIE_HELLMAN", "line_text_before_3": "RIPEMD160", "line_text_after_1": "KECCAK", "line_text_after_2": "SCRYPT", "line_text_after_3": "SHA384", "evidence_type": "algorithm/asymmetric/ECC", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "SHA384", "line_text": "SHA384", "line_number": 26, "file_index_begin": 213, "file_index_end": 219, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "SCRYPT", "line_text_before_2": "KECCAK", "line_text_before_3": "ECDSA", "line_text_after_1": "DES", "line_text_after_2": "STREAMCIPHER", "line_text_after_3": "AES128", "evidence_type": "algorithm/hash/SHA2", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "AES128", "line_text": "AES128", "line_number": 29, "file_index_begin": 237, "file_index_end": 243, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "STREAMCIPHER", "line_text_before_2": "DES", "line_text_before_3": "SHA384", "line_text_after_1": "AES256", "line_text_after_2": "DES_EDE", "line_text_after_3": "SHA224", "evidence_type": "algorithm/symmetric/block-cipher/AES", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "AES256", "line_text": "AES256", "line_number": 30, "file_index_begin": 244, "file_index_end": 250, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "AES128", "line_text_before_2": "STREAMCIPHER", "line_text_before_3": "DES", "line_text_after_1": "DES_EDE", "line_text_after_2": "SHA224", "line_text_after_3": "SHA512", "evidence_type": "algorithm/symmetric/block-cipher/AES", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "DES_", "line_text": "DES_EDE", "line_number": 31, "file_index_begin": 251, "file_index_end": 255, "line_index_begin": 0, "line_index_end": 4, "line_text_before_1": "AES256", "line_text_before_2": "AES128", "line_text_before_3": "STREAMCIPHER", "line_text_after_1": "SHA224", "line_text_after_2": "SHA512", "line_text_after_3": "SHA1", "evidence_type": "algorithm/symmetric/block-cipher/DES", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "SHA224", "line_text": "SHA224", "line_number": 32, "file_index_begin": 259, "file_index_end": 265, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "DES_EDE", "line_text_before_2": "AES256", "line_text_before_3": "AES128", "line_text_after_1": "SHA512", "line_text_after_2": "SHA1", "line_text_after_3": "DSA", "evidence_type": "algorithm/hash/SHA2", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "SHA512", "line_text": "SHA512", "line_number": 33, "file_index_begin": 266, "file_index_end": 272, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "SHA224", "line_text_before_2": "DES_EDE", "line_text_before_3": "AES256", "line_text_after_1": "SHA1", "line_text_after_2": "DSA", "line_text_after_3": "1.2.840.10045.3.1.1", "evidence_type": "algorithm/hash/SHA2", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "SHA1", "line_text": "SHA1", "line_number": 34, "file_index_begin": 273, "file_index_end": 277, "line_index_begin": 0, "line_index_end": 4, "line_text_before_1": "SHA512", "line_text_before_2": "SHA224", "line_text_before_3": "DES_EDE", "line_text_after_1": "DSA", "line_text_after_2": "1.2.840.10045.3.1.1", "line_text_after_3": "SECP521R1", "evidence_type": "algorithm/hash/SHA1", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "1.2.840.10045.3.1.1", "line_text": "1.2.840.10045.3.1.1", "line_number": 36, "file_index_begin": 282, "file_index_end": 301, "line_index_begin": 0, "line_index_end": 19, "line_text_before_1": "DSA", "line_text_before_2": "SHA1", "line_text_before_3": "SHA512", "line_text_after_1": "SECP521R1", "line_text_after_2": "SECP256R1", "line_text_after_3": "SECP192R1", "evidence_type": "algorithm/asymmetric/ECC", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}, {"matched_text": "RIPEMD", "line_text": "RIPEMD", "line_number": 43, "file_index_begin": 355, "file_index_end": 361, "line_index_begin": 0, "line_index_end": 6, "line_text_before_1": "SSH", "line_text_before_2": "PKCS", "line_text_before_3": "DIFFIEHELLMAN", "line_text_after_1": "RSAPRIVATEKEY", "line_text_after_2": "RSAPUBLICKEY", "line_text_after_3": "DSAPRIVATEKEY", "evidence_type": "algorithm/hash/RIPEMD", "detection_method": "keyword", "comments": "", "human_reviewed": "", "encryption_api_usage": "", "encryption_library": ""}], "is_source_code":

false}}}