The CVE with id CVE-2021-45929 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.057 and modified on date 2022-01-10T13:06:50.350. The vulnerability is described as Wasm3 0.5.0 has an out-of-bounds write in CompileBlock (called from CompileElseBlock and Compile_If).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45944 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.183 and modified on date 2022-01-21T14:41:26.383. The vulnerability is described as Ghostscript GhostPDL 9.50 through 9.53.3 has a use-after-free in sampled_data_sample (called from sampled_data_continue and interp).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45945 and source identifier N/A was originally published on date 2022-01-01T00:15:08.230 and modified on date 2022-01-17T22:15:08.430. The vulnerability is described as ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.. It has severity N/A with exploitability score N/A and impact score N/A.

The CVE with id CVE-2021-45946 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.277 and modified on date 2022-01-10T13:06:53.497. The vulnerability is described as Wasm3 0.5.0 has an out-of-bounds write in CompileBlock (called from Compile_LoopOrBlock and CompileBlockStatements).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45947 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.320 and modified on date 2022-01-10T13:06:45.430. The vulnerability is described as Wasm3 0.5.0 has an out-of-bounds write in Runtime_Release (called from EvaluateExpression and InitDataSegments).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45948 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.367 and modified on date 2022-10-28T20:10:04.987. The vulnerability is described as Open Asset Import Library (aka assimp) 5.1.0 and 5.1.1 has a heap-based buffer overflow in _m3d_safestr (called from m3d_load and Assimp::M3DWrapper::M3DWrapper).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45949 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.413 and modified on date 2022-01-21T14:41:34.540. The vulnerability is described as Ghostscript GhostPDL 9.50 through 9.54.0 has a heap-based buffer overflow in sampled_data_finish (called from sampled_data_continue and interp).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45950 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.460 and modified on date 2022-01-11T16:00:25.127. The vulnerability is described as LibreDWG 0.12.4.4313 through 0.12.4.4367 has an out-of-bounds write in dwg_free_BLOCK_private (called from dwg_free_BLOCK and dwg_free_object).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45951 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.507 and modified on date 2022-03-18T13:17:37.490. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in check_bad_address (called from check_for_bogus_wildcard and FuzzCheckForBogusWildcard). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.". It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45952 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.553 and modified on date 2022-03-18T13:20:04.737. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in dhcp_reply (called from dhcp_packet and FuzzDhcp). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.". It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45953 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.593 and modified on date 2022-03-18T13:25:08.600. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in extract_name (called from hash_questions and fuzz_util.c). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.". It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45954 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.637 and modified on date 2022-03-18T13:32:08.650. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in extract_name (called from answer_auth and FuzzAuth). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.". It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45955 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.677 and modified on date 2022-03-18T13:33:15.280. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in resize_packet (called from FuzzResizePacket and fuzz_rfc1035.c) because of the lack of a proper bounds check upon pseudo header re-insertion. NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge." However, a contributor states that a security patch (mentioned in 016162.html) is needed.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45956 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.720 and modified on date 2022-03-18T13:32:50.287. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in print_mac (called from log_packet and dhcp_reply). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.". It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45957 and source identifier nvd@nist.gov was originally published on

date 2022-01-01T00:15:08.767 and modified on date 2022-03-18T13:31:43.057. The vulnerability is described as ** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in answer_request (called from FuzzAnswerTheRequest and fuzz_rfc1035.c). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.". It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45958 and source identifier nvd@nist.gov was originally published on date 2022-01-01T00:15:08.813 and modified on date 2022-09-10T02:38:59.120. The vulnerability is described as UltraJSON (aka ujson) through 5.1.0 has a stack-based buffer overflow in Buffer_AppendIndentUnchecked (called from encode). Exploitation can, for example, use a large amount of indentation.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45959 and source identifier N/A was originally published on date 2022-01-01T00:15:08.860 and modified on date 2022-01-03T08:15:09.283. The vulnerability is described as ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.. It has severity N/A with exploitability score N/A and impact score N/A.

The CVE with id CVE-2021-45926 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.263 and modified on date 2022-12-09T16:39:31.917. The vulnerability is described as MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd0c689be0) in mdb_numeric_to_string (called from mdb_xfer_bound_data and _mdb_attempt_bind).. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-45927 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.317 and modified on date 2022-12-09T16:40:49.057. The vulnerability is described as MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd6e029ee0) in mdb_numeric_to_string (called from mdb_xfer_bound_data and _mdb_attempt_bind).. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-45928 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.367 and modified on date 2022-01-12T14:31:35.367. The vulnerability is described as libjxl b02d6b9, as used in libvips 8.11 through 8.11.2 and other products, has an out-of-bounds write in jxl::ModularFrameDecoder::DecodeGroup (called from jxl::FrameDecoder::ProcessACGroup and jxl::ThreadPool::RunCallState<jxl::FrameDecoder::ProcessSections).. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-45930 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.420 and modified on date 2022-02-10T14:52:17.643. The vulnerability is described as Qt SVG in Qt 5.0.0 through 5.15.2 and 6.0.0 through 6.2.1 has an out-of-bounds write in QtPrivate::QCommonArrayOps<QPainterPath::Element>::growAppend (called from QPainterPath::addPath and QPathClipper::intersect).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45931 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.477 and modified on date 2022-10-28T12:54:22.913. The vulnerability is

described as HarfBuzz 2.9.0 has an out-of-bounds write in hb_bit_set_invertible_t::set (called from hb_sparseset_t<hb_bit_set_invertible_t>::set and hb_set_copy).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45932 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.527 and modified on date 2022-01-11T21:11:53.800. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow (4 bytes) in MqttDecode_Publish (called from MqttClient_DecodePacket and MqttClient_HandlePacket).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45933 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.577 and modified on date 2022-01-11T21:12:44.410. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow (8 bytes) in MqttDecode_Publish (called from MqttClient_DecodePacket and MqttClient_HandlePacket).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45934 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.630 and modified on date 2022-01-11T21:14:55.067. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_HandlePacket and MqttClient_WaitType).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45935 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.680 and modified on date 2022-01-11T18:54:32.083. The vulnerability is described as Grok 9.5.0 has a heap-based buffer overflow in openhtj2k::T1OpenHTJ2K::decompress (called from std::__1::__packaged_task_func<std::__1::__bind<grk::T1DecompressScheduler::deco and std::__1::packaged_task<int).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45936 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.730 and modified on date 2022-01-11T21:16:44.447. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttDecode_Disconnect (called from MqttClient_DecodePacket and MqttClient_WaitType).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45937 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.780 and modified on date 2022-01-11T21:17:38.743. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Connect).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45938 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.833 and modified on date 2022-01-11T21:20:55.207. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Unsubscribe).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45939 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.887 and modified on date 2022-01-11T21:22:11.023. The vulnerability is described as wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Subscribe).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45940 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.940 and modified on date 2022-01-11T18:20:25.707. The vulnerability is described as libbpf 0.6.0 and 0.6.1 has a heap-based buffer overflow (4 bytes) in __bpf_object__open (called from bpf_object__open_mem and bpf-object-fuzzer.c).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45941 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:08.990 and modified on date 2022-01-11T18:18:24.910. The vulnerability is described as libbpf 0.6.0 and 0.6.1 has a heap-based buffer overflow (8 bytes) in __bpf_object__open (called from bpf_object__open_mem and bpf-object-fuzzer.c).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45942 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:09.043 and modified on date 2023-02-03T23:34:41.300. The vulnerability is described as OpenEXR 3.1.x before 3.1.4 has a heap-based buffer overflow in Imf_3_1::LineCompositeTask::execute (called from IlmThread_3_1::NullThreadPoolProvider::addTask and IlmThread_3_1::ThreadPool::addGlobalTask). NOTE: db217f2 may be inapplicable.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45943 and source identifier nvd@nist.gov was originally published on date 2022-01-01T01:15:09.100 and modified on date 2022-11-04T15:49:23.800. The vulnerability is described as GDAL 3.3.0 through 3.4.0 has a heap-based buffer overflow in PCIDSK::CPCIDSKFile::ReadFromFile (called from PCIDSK::CPCIDSKSegment::ReadFromFile and PCIDSK::CPCIDSKBinarySegment::CPCIDSKBinarySegment).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-41817 and source identifier nvd@nist.gov was originally published on date 2022-01-01T05:15:08.197 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as Date.parse in the date gem through 3.2.0 for Ruby allows ReDoS (regular expression Denial of Service) via a long string. The fixed versions are 3.2.1, 3.1.2, 3.0.2, and 2.0.1.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-44716 and source identifier nvd@nist.gov was originally published on date 2022-01-01T05:15:08.307 and modified on date 2023-04-20T00:15:07.663. The vulnerability is described as net/http in Go before 1.16.12 and 1.17.x before 1.17.5 allows uncontrolled memory consumption in the header canonicalization cache via HTTP/2 requests.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-44717 and source identifier nvd@nist.gov was originally published on

date 2022-01-01T05:15:08.367 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as Go before 1.16.12 and 1.17.x before 1.17.5 on UNIX allows write operations to an unintended file or unintended network connection as a consequence of erroneous closing of file descriptor 0 after file-descriptor exhaustion.. It has severity MEDIUM with exploitability score 8.6 and impact score 4.9.

The CVE with id CVE-2021-41819 and source identifier nvd@nist.gov was originally published on date 2022-01-01T06:15:07.293 and modified on date 2022-09-10T02:39:25.880. The vulnerability is described as CGI::Cookie.parse in Ruby through 2.6.8 mishandles security prefixes in cookie names. This also affects the CGI gem through 0.3.0 for Ruby.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-43333 and source identifier nvd@nist.gov was originally published on date 2022-01-01T06:15:07.397 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as The Datalogic DXU service on (for example) DL-Axist devices does not require authentication for configuration changes or disclosure of configuration settings.. It has severity MEDIUM with exploitability score 8.6 and impact score 4.9.

The CVE with id CVE-2021-44852 and source identifier nvd@nist.gov was originally published on date 2022-01-01T06:15:07.453 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as An issue was discovered in BS_RCIO64.sys in Biostar RACING GT Evo 2.1.1905.1700. A low-integrity process can open the driver's device object and issue IOCTLs to read or write to arbitrary physical memory locations (or call an arbitrary address), leading to execution of arbitrary code. This is associated with 0x226040, 0x226044, and 0x226000.. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-45960 and source identifier nvd@nist.gov was originally published on date 2022-01-01T19:15:08.030 and modified on date 2022-10-06T19:08:03.287. The vulnerability is described as In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).. It has severity HIGH with exploitability score 8.0 and impact score 10.0.

The CVE with id CVE-2021-45972 and source identifier nvd@nist.gov was originally published on date 2022-01-01T21:15:07.730 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as The giftrans function in giftrans 1.12.2 contains a stack-based buffer overflow because a value inside the input file determines the amount of data to write. This allows an attacker to overwrite up to 250 bytes outside of the allocated buffer with arbitrary data.. It has severity MEDIUM with exploitability score 8.6 and impact score 4.9.

The CVE with id CVE-2021-44896 and source identifier nvd@nist.gov was originally published on date 2022-01-01T23:15:08.647 and modified on date 2022-01-07T19:39:18.350. The vulnerability is described as DMP Roadmap before 3.0.4 allows XSS.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-22293 and source identifier nvd@nist.gov was originally published on date 2022-01-02T00:15:09.673 and modified on date 2022-11-17T17:21:59.260. The vulnerability is described as admin/limits.php in Dolibarr 7.0.2 allows HTML injection, as demonstrated by the

MAIN_MAX_DECIMALS_TOT parameter.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2022-0080 and source identifier nvd@nist.gov was originally published on date 2022-01-02T12:15:07.690 and modified on date 2022-01-11T14:22:16.563. The vulnerability is described as mruby is vulnerable to Heap-based Buffer Overflow. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-36751 and source identifier nvd@nist.gov was originally published on date 2022-01-02T16:15:07.860 and modified on date 2022-12-13T19:30:07.903. The vulnerability is described as ENC DataVault 7.2.3 and before, and OEM versions, use an encryption algorithm that is vulnerable to data manipulation (without knowledge of the key). This is called ciphertext malleability. There is no data integrity mechanism to detect this manipulation.. It has severity MEDIUM with exploitability score 10.0 and impact score 4.9.

The CVE with id CVE-2022-0079 and source identifier nvd@nist.gov was originally published on date 2022-01-03T03:15:07.013 and modified on date 2022-01-10T21:29:24.020. The vulnerability is described as showdoc is vulnerable to Generation of Error Message Containing Sensitive Information. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-25981 and source identifier nvd@nist.gov was originally published on date 2022-01-03T07:15:06.943 and modified on date 2022-01-14T18:26:51.553. The vulnerability is described as In Talkyard, regular versions v0.2021.20 through v0.2021.33 and dev versions v0.2021.20 through v0.2021.34, are vulnerable to Insufficient Session Expiration. This may allow an attacker to reuse the admin’s still-valid session token even when logged-out, to gain admin privileges, given the attacker is able to obtain that token (via other, hypothetical attacks). It has severity HIGH with exploitability score 10.0 and impact score 10.0.

The CVE with id CVE-2021-25994 and source identifier nvd@nist.gov was originally published on date 2022-01-03T07:15:07.243 and modified on date 2022-01-13T17:43:02.343. The vulnerability is described as In Userfrosting, versions v0.3.1 to v4.6.2 are vulnerable to Host Header Injection. By luring a victim application user to click on a link, an unauthenticated attacker can use the “forgot password” functionality to reset the victim’s password and successfully take over their account.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2020-11263 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.497 and modified on date 2022-01-11T15:17:13.420. The vulnerability is described as An integer overflow due to improper check performed after the address and size passed are aligned in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-1894 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.587 and modified on date 2022-01-12T16:58:16.060. The vulnerability is described as Improper access control in TrustZone due to improper error handling while handling the signing key in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired

Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-1918 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.650 and modified on date 2022-01-11T15:19:05.383. The vulnerability is described as Improper handling of resource allocation in virtual machines can lead to information exposure in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-30262 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.717 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as Improper validation of a socket state when socket events are being sent to clients can lead to invalid access of memory in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-30267 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.777 and modified on date 2022-01-11T16:12:29.453. The vulnerability is described as Possible integer overflow to buffer overflow due to improper input validation in FTM ARA commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-30268 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.833 and modified on date 2022-01-12T17:00:10.520. The vulnerability is described as Possible heap Memory Corruption Issue due to lack of input validation when sending HWTC IQ Capture command in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30269 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.897 and modified on date 2022-01-12T17:03:18.357. The vulnerability is described as Possible null pointer dereference due to lack of TLB validation for user provided address in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30270 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:07.957 and modified on date 2022-01-12T16:09:29.837. The vulnerability is described as Possible null pointer dereference in thread profile trap handler due to lack of thread ID validation before dereferencing it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30271 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.017 and modified on date 2022-01-12T16:18:09.963. The vulnerability is described as Possible null pointer dereference in trap handler due to lack of thread ID validation before dereferencing it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30272 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.073 and modified on date 2022-01-12T16:39:40.190. The vulnerability is described as Possible null pointer dereference in thread cache operation handler due to lack of validation of user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30273 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.133 and modified on date 2022-01-11T21:33:36.267. The vulnerability is described as Possible assertion due to improper handling of IPV6 packet with invalid length in destination options header in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-30274 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.197 and modified on date 2022-01-12T14:49:20.323. The vulnerability is described as Possible integer overflow in access control initialization interface due to lack and size and address validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30275 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.257 and modified on date 2022-01-12T14:46:25.887. The vulnerability is described as Possible integer overflow in page alignment interface due to lack of address and size validation before alignment in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30276 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.317 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as Improper access control while doing XPU re-configuration dynamically can lead to unauthorized access to a secure resource in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30278 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.377 and modified on date 2022-01-12T14:55:58.173. The vulnerability is described as Improper input validation in TrustZone memory transfer interface can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-30279 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.433 and modified on date 2022-01-12T15:13:17.840. The vulnerability is described as Possible access control violation while setting current permission for VMIDs due to improper permission masking in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30282 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.490 and modified on date 2022-01-12T15:26:38.393. The vulnerability is described as Possible out of bound write in RAM partition table due to improper validation on number of partitions provided in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30283 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.550 and modified on date 2022-01-12T17:58:40.500. The vulnerability is described as Possible denial of service due to improper handling of debug register trap from user applications in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-30289 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.610 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as Possible buffer overflow due to lack of range check while processing a DIAG command for COEX management in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30293 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.667 and modified on date 2022-01-12T15:30:07.253. The vulnerability is described as Possible assertion due to lack of input validation in PUSCH configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-30298 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.727 and modified on date 2022-01-12T15:41:57.967. The vulnerability is described as Possible out of bound access due to improper validation of item size and DIAG

memory pools data while switching between USB and PCIE interface in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-30303 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.787 and modified on date 2022-01-12T15:42:51.590. The vulnerability is described as Possible buffer overflow due to lack of buffer length check when segmented WMI command is received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30335 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.843 and modified on date 2022-01-12T15:48:42.547. The vulnerability is described as Possible assertion in QOS request due to improper validation when multiple add or update request are received simultaneously in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30336 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.903 and modified on date 2022-01-12T15:53:33.353. The vulnerability is described as Possible out of bound read due to lack of domain input validation while processing APK close session request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30337 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:08.960 and modified on date 2022-01-12T15:54:28.927. The vulnerability is described as Possible use after free when process shell memory is freed using IOCTL call and process initialization is in progress in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-30348 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:09.020 and modified on date 2022-01-12T15:58:35.747. The vulnerability is described as Improper validation of LLM utility timers availability can lead to denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2021-30351 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:09.080 and modified on date 2022-01-12T15:27:43.880. The vulnerability is described as An out of bound memory access can occur due to improper validation of number of

frames being passed during music playback in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-35093 and source identifier nvd@nist.gov was originally published on date 2022-01-03T08:15:09.147 and modified on date 2022-01-13T17:35:41.893. The vulnerability is described as Possible memory corruption in BT controller when it receives an oversized LMP packet over 2-DH1 link and leads to denial of service in BlueCore. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2021-44158 and source identifier nvd@nist.gov was originally published on date 2022-01-03T10:15:08.190 and modified on date 2023-06-26T19:02:59.217. The vulnerability is described as ASUS RT-AX56U Wi-Fi Router is vulnerable to stack-based buffer overflow due to improper validation for httpd parameter length. An authenticated local area network attacker can launch arbitrary code execution to control the system or disrupt service.. It has severity HIGH with exploitability score 5.1 and impact score 10.0.

The CVE with id CVE-2021-45916 and source identifier nvd@nist.gov was originally published on date 2022-01-03T10:15:08.327 and modified on date 2022-01-11T18:49:46.210. The vulnerability is described as The programming function of Shockwall system has an improper input validation vulnerability. An authenticated attacker within the local area network can send malicious response to the server to disrupt the service partially.. It has severity LOW with exploitability score 5.1 and impact score 2.9.

The CVE with id CVE-2021-45917 and source identifier nvd@nist.gov was originally published on date 2022-01-03T10:15:08.390 and modified on date 2022-01-07T19:41:59.400. The vulnerability is described as The server-request receiver function of Shockwall system has an improper authentication vulnerability. An authenticated attacker of an agent computer within the local area network can use the local registry information to launch server-side request forgery (SSRF) attack on another agent computer, resulting in arbitrary code execution for controlling the system or disrupting service.. It has severity HIGH with exploitability score 5.1 and impact score 10.0.

The CVE with id CVE-2021-24680 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.090 and modified on date 2022-01-07T19:42:54.427. The vulnerability is described as The WP Travel Engine WordPress plugin before 5.3.1 does not escape the Description field in the Trip Destination/Activities/Trip Type and Pricing Category pages, allowing users with a role as low as editor to perform Stored Cross-Site Scripting attacks, even when the unfiltered_html capability is disallowed. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-24786 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.150 and modified on date 2022-01-11T14:56:22.397. The vulnerability is described as The Download Monitor WordPress plugin before 4.4.5 does not properly validate and escape the "orderby" GET parameter before using it in a SQL statement when viewing the logs, leading to an SQL Injection issue. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-24828 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.210 and modified on date 2022-01-07T19:43:33.533. The vulnerability is described as The Mortgage Calculator / Loan Calculator WordPress plugin before 1.5.17 does not escape the some of the attributes of its mlcalc shortcode before outputting them, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-24831 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.263 and modified on date 2022-02-10T15:11:31.953. The vulnerability is described as All AJAX actions of the Tab WordPress plugin before 1.3.2 are available to both unauthenticated and authenticated users, allowing unauthenticated attackers to modify various data in the plugin, such as add/edit/delete arbitrary tabs.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-24893 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.317 and modified on date 2022-08-30T15:52:01.040. The vulnerability is described as The Stars Rating WordPress plugin before 3.5.1 does not validate the submitted rating, allowing submission of long integer, causing a Denial of Service in the comments section, or pending comment dashboard depending if the user sent it as unauthenticated or authenticated.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-24963 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.457 and modified on date 2022-01-08T02:21:28.663. The vulnerability is described as The LiteSpeed Cache WordPress plugin before 4.4.4 does not escape the qc_res parameter before outputting it back in the JS code of an admin page, leading to a Reflected Cross-Site Scripting. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-24964 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.517 and modified on date 2022-01-08T02:21:59.510. The vulnerability is described as The LiteSpeed Cache WordPress plugin before 4.4.4 does not properly verify that requests are coming from QUIC.cloud servers, allowing attackers to make requests to certain endpoints by using a specific X-Forwarded-For header value. In addition, one of the endpoint could be used to set CSS code if a setting is enabled, which will then be output in some pages without being sanitised and escaped. Combining those two issues, an unauthenticated attacker could put Cross-Site Scripting payloads in pages visited by users.. It has severity LOW with exploitability score 4.9 and impact score 2.9.

The CVE with id CVE-2021-24973 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.570 and modified on date 2022-01-08T02:22:19.283. The vulnerability is described as The Site Reviews WordPress plugin before 5.17.3 does not sanitise and escape the site-reviews parameter of the glsr_action AJAX action (available to unauthenticated and any authenticated users), allowing them to perform Cross-Site Scripting attacks against logged in admins viewing the Tool dashboard of the plugin. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-24991 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.627 and modified on date 2022-01-08T02:30:04.543. The vulnerability is

described as The WooCommerce PDF Invoices & Packing Slips WordPress plugin before 2.10.5 does not escape the tab and section parameters before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting in the admin dashboard. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-24999 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.693 and modified on date 2022-01-08T02:30:40.323. The vulnerability is described as The Booster for WooCommerce WordPress plugin before 5.4.9 does not sanitise and escape the wcj_notice parameter before outputting it back in the admin dashboard when the Pdf Invoicing module is enabled, leading to a Reflected Cross-Site Scripting. It has severity LOW with exploitability score 4.9 and impact score 2.9.

The CVE with id CVE-2021-25000 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.763 and modified on date 2022-01-08T02:35:12.540. The vulnerability is described as The Booster for WooCommerce WordPress plugin before 5.4.9 does not sanitise and escape the wcj_delete_role parameter before outputting back in the admin dashboard when the General module is enabled, leading to a Reflected Cross-Site Scripting issue. It has severity LOW with exploitability score 4.9 and impact score 2.9.

The CVE with id CVE-2021-25001 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.833 and modified on date 2022-01-08T02:39:19.143. The vulnerability is described as The Booster for WooCommerce WordPress plugin before 5.4.9 does not sanitise and escape the wcj_create_products_xml_result parameter before outputting back in the admin dashboard when the Product XML Feeds module is enabled, leading to a Reflected Cross-Site Scripting issue. It has severity LOW with exploitability score 4.9 and impact score 2.9.

The CVE with id CVE-2021-25016 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.890 and modified on date 2022-01-08T02:39:40.863. The vulnerability is described as The Chaty WordPress plugin before 2.8.3 and Chaty Pro WordPress plugin before 2.8.2 do not sanitise and escape the search parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-25020 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:08.957 and modified on date 2022-01-11T13:27:46.867. The vulnerability is described as The CAOS | Host Google Analytics Locally WordPress plugin before 4.1.9 does not validate the cache directory setting, allowing high privilege users to use a path traversal vector and delete arbitrary folders when uninstalling the plugin. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-25021 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.017 and modified on date 2022-01-11T13:28:44.413. The vulnerability is described as The OMGF | Host Google Fonts Locally WordPress plugin before 4.5.12 does not validate the cache directory setting, allowing high privilege users to use a path traversal vector and delete arbitrary folders when uninstalling the plugin. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-25022 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.077 and modified on date 2022-01-08T02:39:59.070. The vulnerability is described as The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.16.66 does not sanitise and escape the backup_timestamp and job_id parameter before outputting then back in admin pages, leading to Reflected Cross-Site Scripting issues. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-25023 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.137 and modified on date 2022-01-11T16:45:15.480. The vulnerability is described as The Speed Booster Pack âš¡ PageSpeed Optimization Suite WordPress plugin before 4.3.3.1 does not escape the sbp_convert_table_name parameter before using it in a SQL statement to convert the related table, leading to an SQL injection. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-25027 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.193 and modified on date 2022-01-08T02:40:33.760. The vulnerability is described as The PowerPack Addons for Elementor WordPress plugin before 2.6.2 does not escape the tab parameter before outputting it back in an attribute in the admin dashboard, leading to a Reflected Cross-Site Scripting issue. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-25030 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.257 and modified on date 2022-01-11T14:27:51.570. The vulnerability is described as The Events Made Easy WordPress plugin before 2.2.36 does not sanitise and escape the search_text parameter before using it in a SQL statement via the eme_searchmail AJAX action, available to any authenticated users. As a result, users with a role as low as subscriber can call it and perform SQL injection attacks. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-25040 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.313 and modified on date 2022-01-08T02:40:49.167. The vulnerability is described as The Booking Calendar WordPress plugin before 8.9.2 does not sanitise and escape the booking_type parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-44674 and source identifier nvd@nist.gov was originally published on date 2022-01-03T13:15:09.997 and modified on date 2022-01-11T16:36:29.893. The vulnerability is described as An information exposure issue has been discovered in Opmantek Open-AudIT 4.2.0. The vulnerability allows an authenticated attacker to read file outside of the restricted directory.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-45428 and source identifier nvd@nist.gov was originally published on date 2022-01-03T14:15:07.693 and modified on date 2022-05-12T19:32:50.973. The vulnerability is described as TLR-2005KSH is affected by an incorrect access control vulnerability. THe PUT method is enabled so an attacker can upload arbitrary files including HTML and CGI formats.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-3837 and source identifier nvd@nist.gov was originally published on date 2022-01-03T15:15:08.480 and modified on date 2022-10-27T11:38:46.010. The vulnerability is described as openwhyd is vulnerable to Improper Authorization. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46109 and source identifier nvd@nist.gov was originally published on date 2022-01-03T15:15:09.097 and modified on date 2022-01-08T02:42:34.243. The vulnerability is described as Invalid input sanitizing leads to reflected Cross Site Scripting (XSS) in ASUS RT-AC52U_B1 3.0.0.4.380.10931 can lead to a user session hijack.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45817 and source identifier N/A was originally published on date 2022-01-03T16:15:07.787 and modified on date 2022-01-04T04:15:07.540. The vulnerability is described as ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-11689. Reason: This candidate is a duplicate of CVE-2018-11689. Notes: All CVE users should reference CVE-2018-11689 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.. It has severity N/A with exploitability score N/A and impact score N/A.

The CVE with id CVE-2020-23026 and source identifier nvd@nist.gov was originally published on date 2022-01-03T20:15:07.780 and modified on date 2022-01-08T02:48:37.603. The vulnerability is described as A NULL pointer dereference in the main() function dhry_1.c of dhrystone 2.1 causes a denial of service (DoS).. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-20147 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:08.503 and modified on date 2022-01-13T16:12:42.683. The vulnerability is described as ManageEngine ADSelfService Plus below build 6116 contains an observable response discrepancy in the UMCP operation of the ChangePasswordAPI. This allows an unauthenticated remote attacker to determine whether a Windows domain user exists.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-20148 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:08.560 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as ManageEngine ADSelfService Plus below build 6116 stores the password policy file for each domain under the html/ web root with a predictable filename based on the domain name. When ADSSP is configured with multiple Windows domains, a user from one domain can obtain the password policy for another domain by authenticating to the service and then sending a request specifying the password policy file of the other domain.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-37098 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:08.933 and modified on date 2022-01-11T18:13:47.937. The vulnerability is described as Hilinksvc service exists a Data Processing Errors vulnerability .Successful exploitation of this vulnerability may cause application crash.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37110 and source identifier nvd@nist.gov was originally published on

date 2022-01-03T22:15:09.000 and modified on date 2022-01-11T19:27:32.067. The vulnerability is described as There is a Timing design defects in Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37111 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.057 and modified on date 2022-01-11T19:31:32.390. The vulnerability is described as There is a Memory leakage vulnerability in Smartphone.Successful exploitation of this vulnerability may cause memory exhaustion.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37112 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.113 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as Hisuite module has a External Control of System or Configuration Setting vulnerability.Successful exploitation of this vulnerability may lead to Firmware leak.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37113 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.170 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as There is a Privilege escalation vulnerability with the file system component in Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37114 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.227 and modified on date 2022-01-11T19:39:59.973. The vulnerability is described as There is an Out-of-bounds read vulnerability in Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37116 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.287 and modified on date 2022-01-11T19:44:30.417. The vulnerability is described as PCManager has a Weaknesses Introduced During Design vulnerability .Successful exploitation of this vulnerability may cause that the PIN of the subscriber is changed.. It has severity MEDIUM with exploitability score 10.0 and impact score 4.9.

The CVE with id CVE-2021-37117 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.347 and modified on date 2022-01-11T19:46:26.163. The vulnerability is described as There is a Service logic vulnerability in Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37118 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.400 and modified on date 2022-01-11T19:52:56.000. The vulnerability is described as The HwNearbyMain module has a Improper Handling of Exceptional Conditions vulnerability.Successful exploitation of this vulnerability may lead to message leak.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37119 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.450 and modified on date 2022-01-11T19:58:15.363. The vulnerability is described as There is a Service logic vulnerability in Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37120 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.500 and modified on date 2022-01-13T15:54:39.633. The vulnerability is described as There is a Double free vulnerability in Smartphone.Successful exploitation of this vulnerability may cause a kernel crash or privilege escalation.. It has severity HIGH with exploitability score 10.0 and impact score 10.0.

The CVE with id CVE-2021-37121 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.550 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as There is a Configuration defects in Smartphone.Successful exploitation of this vulnerability may elevate the MEID (IMEI) permission.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-37125 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.597 and modified on date 2022-01-13T16:17:25.327. The vulnerability is described as Arbitrary file has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability .Successful exploitation of this vulnerability may cause confidentiality is affected.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37126 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.643 and modified on date 2022-01-11T20:04:44.400. The vulnerability is described as Arbitrary file has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability .Successful exploitation of this vulnerability may cause the directory is traversed.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37128 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.690 and modified on date 2022-01-11T20:05:38.820. The vulnerability is described as HwPCAssistant has a Path Traversal vulnerability .Successful exploitation of this vulnerability may write any file.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-37132 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.747 and modified on date 2022-01-11T20:06:28.397. The vulnerability is described as PackageManagerService has a Permissions, Privileges, and Access Controls vulnerability .Successful exploitation of this vulnerability may cause that Third-party apps can obtain the complete list of Harmony apps without permission.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37133 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.800 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as There is an Unauthorized file access vulnerability in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with

exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-37134 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.857 and modified on date 2022-01-13T16:18:19.047. The vulnerability is described as Location-related APIs exists a Race Condition vulnerability.Successful exploitation of this vulnerability may use Higher Permissions for invoking the interface of location-related components.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-38576 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.903 and modified on date 2022-01-13T16:21:04.917. The vulnerability is described as A BIOS bug in firmware for a particular PC model leaves the Platform authorization value empty. This can be used to permanently brick the TPM in multiple ways, as well as to non-permanently DoS the system.. It has severity HIGH with exploitability score 10.0 and impact score 6.9.

The CVE with id CVE-2021-39966 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:09.957 and modified on date 2022-01-13T16:22:11.833. The vulnerability is described as There is an Uninitialized AOD driver structure in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39967 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.000 and modified on date 2022-01-13T16:23:38.167. The vulnerability is described as There is a Vulnerability of obtaining broadcast information improperly due to improper broadcast permission settings in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39968 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.047 and modified on date 2022-01-13T16:28:17.993. The vulnerability is described as Changlian Blocklist has a Business Logic Errors vulnerability .Successful exploitation of this vulnerability may expand the attack surface of the message class.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39969 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.093 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as There is an Unauthorized file access vulnerability in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39970 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.140 and modified on date 2022-01-13T15:46:21.260. The vulnerability is described as HwPCAssistant has a Improper Input Validation vulnerability.Successful exploitation of this vulnerability may create any file with the system app permission.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39971 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.190 and modified on date 2023-08-08T14:21:49.707. The vulnerability is

described as Password vault has a External Control of System or Configuration Setting vulnerability.Successful exploitation of this vulnerability could compromise confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39972 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.237 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as MyHuawei-App has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability.Successful exploitation of this vulnerability could compromise confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39973 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.283 and modified on date 2022-01-13T15:52:06.580. The vulnerability is described as There is a Null pointer dereference in Smartphones.Successful exploitation of this vulnerability may cause the kernel to break down.. It has severity HIGH with exploitability score 10.0 and impact score 6.9.

The CVE with id CVE-2021-39974 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.333 and modified on date 2022-01-13T15:52:46.770. The vulnerability is described as There is an Out-of-bounds read in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39975 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.380 and modified on date 2022-01-13T16:02:44.597. The vulnerability is described as Hilinksvc has a Data Processing Errors vulnerability.Successful exploitation of this vulnerability may cause denial of service attacks.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39977 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.427 and modified on date 2022-01-13T15:59:36.237. The vulnerability is described as The HwNearbyMain module has a NULL Pointer Dereference vulnerability.Successful exploitation of this vulnerability may cause a process to restart.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39978 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.473 and modified on date 2022-01-13T15:44:20.833. The vulnerability is described as Telephony application has a SQL Injection vulnerability.Successful exploitation of this vulnerability may cause privacy and security issues.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39979 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.523 and modified on date 2022-01-13T15:39:19.687. The vulnerability is described as HHEE system has a Code Injection vulnerability.Successful exploitation of this vulnerability may affect HHEE system integrity.. It has severity HIGH with exploitability score 10.0 and impact score 10.0.

The CVE with id CVE-2021-39980 and source identifier nvd@nist.gov was originally published on

date 2022-01-03T22:15:10.570 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as Telephony application has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability.Successful exploitation of this vulnerability could lead to sensitive information disclosure.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39981 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.627 and modified on date 2022-01-13T19:21:58.607. The vulnerability is described as Chang Lian application has a vulnerability which can be maliciously exploited to hide the calling number.Successful exploitation of this vulnerability allows you to make an anonymous call.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-39982 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.687 and modified on date 2022-01-13T19:28:23.277. The vulnerability is described as Phone Manager application has a Improper Privilege Management vulnerability.Successful exploitation of this vulnerability may read and write arbitrary files by tampering with Phone Manager notifications.. It has severity MEDIUM with exploitability score 10.0 and impact score 4.9.

The CVE with id CVE-2021-39983 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.747 and modified on date 2022-01-13T17:37:31.923. The vulnerability is described as The HwNearbyMain module has a Data Processing Errors vulnerability.Successful exploitation of this vulnerability may cause a process to restart.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39984 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.793 and modified on date 2022-01-13T17:40:23.130. The vulnerability is described as Huawei idap module has a Out-of-bounds Read vulnerability.Successful exploitation of this vulnerability may cause Denial of Service.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39985 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.843 and modified on date 2022-01-14T15:32:12.377. The vulnerability is described as The HwNearbyMain module has a Improper Validation of Array Index vulnerability.Successful exploitation of this vulnerability may cause a process to restart.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39987 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.890 and modified on date 2022-01-14T15:51:23.237. The vulnerability is described as The HwNearbyMain module has a Data Processing Errors vulnerability.Successful exploitation of this vulnerability may cause a process to restart.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39988 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.937 and modified on date 2022-01-14T15:56:02.800. The vulnerability is described as The HwNearbyMain module has a NULL Pointer Dereference vulnerability.Successful exploitation of this vulnerability may cause a process to restart.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39989 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:10.980 and modified on date 2022-01-14T16:00:42.303. The vulnerability is described as The HwNearbyMain module has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability.Successful exploitation of this vulnerability may cause a process to restart.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39990 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:11.030 and modified on date 2022-01-14T16:04:15.630. The vulnerability is described as The screen lock module has a Stack-based Buffer Overflow vulnerability.Successful exploitation of this vulnerability may affect user experience.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45829 and source identifier nvd@nist.gov was originally published on date 2022-01-03T22:15:11.153 and modified on date 2022-01-11T16:37:21.193. The vulnerability is described as HDF5 1.13.1-1 is affected by: segmentation fault, which causes a Denial of Service.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-43942 and source identifier nvd@nist.gov was originally published on date 2022-01-04T03:15:07.233 and modified on date 2022-03-28T13:34:02.910. The vulnerability is described as Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Reflected Cross-Site Scripting (XSS) vulnerability in the /rest/collectors/1.0/template/custom endpoint. To exploit this issue, the attacker must trick a user into visiting a malicious website. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-20868 and source identifier nvd@nist.gov was originally published on date 2022-01-04T04:15:07.270 and modified on date 2022-01-21T14:48:57.470. The vulnerability is described as Incorrect authorization vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, and bizhub 4752/4052 GC9-X4 and earlier) allows an attacker on the adjacent network to obtain user credentials if external server authentication is enabled via a specific SOAP message sent by an administrative user.. It has severity LOW with exploitability score 4.4 and impact score 2.9.

The CVE with id CVE-2021-20869 and source identifier nvd@nist.gov was originally published on date 2022-01-04T04:15:07.323 and modified on date 2022-01-13T02:57:50.150. The vulnerability is described as Exposure of sensitive information to an unauthorized actor vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, and bizhub 4752/4052 GC9-X4 and earlier) allows an attacker on the adjacent network to obtain some of user credentials if LDAP server authentication is enabled via a specific SOAP message.. It has severity LOW with exploitability score 5.5 and impact score 2.9.

The CVE with id CVE-2021-20870 and source identifier nvd@nist.gov was originally published on date 2022-01-04T04:15:07.367 and modified on date 2022-01-13T12:44:33.653. The vulnerability is described as Improper handling of exceptional conditions vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, bizhub 4752/4052 GC9-X4 and earlier, bizhub C3850/C3350/3850FS, bizhub 4750/4050, bizhub C3110, bizhub C3100P) allows a physical attacker to obtain unsent scanned image data when scanned data transmission is stopped due to the network error by ejecting a HDD before the scan job times out.. It has severity LOW with exploitability score 3.4 and impact score 2.9.

The CVE with id CVE-2021-20871 and source identifier nvd@nist.gov was originally published on date 2022-01-04T04:15:07.413 and modified on date 2022-01-13T14:11:57.947. The vulnerability is described as Exposure of sensitive information to an unauthorized actor vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and

earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, and bizhub 4752/4052 GC9-X4 and earlier) allows an attacker on the adjacent network to obtain the credentials if the destination information including credentials are registered in the address book via a specific SOAP message.. It has severity LOW with exploitability score 5.5 and impact score 2.9.

The CVE with id CVE-2021-20872 and source identifier nvd@nist.gov was originally published on date 2022-01-04T04:15:07.457 and modified on date 2022-01-13T13:33:45.353. The vulnerability is described as Protection mechanism failure vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, bizhub 4752/4052 GC9-X4 and earlier) allows a physical attacker to bypass the firmware integrity verification and to install malicious firmware.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2022-0083 and source identifier nvd@nist.gov was originally published on date 2022-01-04T07:15:07.153 and modified on date 2022-01-11T20:09:15.753. The vulnerability is described as livehelperchat is vulnerable to Generation of Error Message Containing Sensitive Information. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-34797 and source identifier nvd@nist.gov was originally published on date 2022-01-04T09:15:07.127 and modified on date 2022-01-12T19:39:06.810. The vulnerability is described as Apache Geode versions up to 1.12.4 and 1.13.4 are vulnerable to a log file redaction of sensitive information flaw when using values that begin with characters other than letters or numbers for passwords and security properties with the prefix "sysprop-", "javax.net.ssl", or "security-". This issue is fixed by overhauling the log file redaction in Apache Geode versions 1.12.5, 1.13.5, and 1.14.0.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-38542 and source identifier nvd@nist.gov was originally published on date 2022-01-04T09:15:07.267 and modified on date 2022-10-27T11:39:19.073. The vulnerability is described as Apache James prior to release 3.6.1 is vulnerable to a buffering attack relying on the use of the STARTTLS command. This can result in Man-in -the-middle command injection attacks, leading potentially to leakage of sensible information.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-40110 and source identifier nvd@nist.gov was originally published on date 2022-01-04T09:15:07.327 and modified on date 2022-01-12T19:54:54.953. The vulnerability is described as In Apache James, using Jazzer fuzzer, we identified that an IMAP user can craft IMAP LIST commands to orchestrate a Denial Of Service using a vulnerable Regular expression. This affected Apache James prior to 3.6.1 We recommend upgrading to Apache James 3.6.1 or higher , which enforce the use of RE2J regular expression engine to execute regex in linear time without back-tracking.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-40111 and source identifier nvd@nist.gov was originally published on date 2022-01-04T09:15:07.377 and modified on date 2022-01-12T20:06:25.853. The vulnerability is described as In Apache James, while fuzzing with Jazzer the IMAP parsing stack, we discover that crafted APPEND and STATUS IMAP command could be used to trigger infinite loops resulting in expensive CPU computations and OutOfMemory exceptions. This can be used for a Denial Of Service attack. The IMAP user needs to be authenticated to exploit this vulnerability. This affected Apache James prior to version 3.6.1. This vulnerability had been patched in Apache James 3.6.1 and higher. We recommend the upgrade.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-40525 and source identifier nvd@nist.gov was originally published on date 2022-01-04T09:15:07.423 and modified on date 2022-03-29T16:34:56.937. The vulnerability is described as Apache James ManagedSieve implementation alongside with the file storage for sieve scripts is vulnerable to path traversal, allowing reading and writing any file. This vulnerability had been patched in Apache James 3.6.1 and higher. We recommend the upgrade. Distributed and Cassandra based products are also not impacted.. It has severity MEDIUM with exploitability score 10.0 and impact score 4.9.

The CVE with id CVE-2021-31833 and source identifier nvd@nist.gov was originally published on date 2022-01-04T10:15:07.977 and modified on date 2022-01-12T21:27:32.037. The vulnerability is described as Potential product security bypass vulnerability in McAfee Application and Change Control (MACC) prior to version 8.3.4 allows a locally logged in attacker to circumvent the application solidification protection provided by MACC, permitting them to run applications that would usually be prevented by MACC. This would require the attacker to rename the specified binary to match name of any configured updater and perform a specific set of steps, resulting in the renamed binary to be to run.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-44168 and source identifier nvd@nist.gov was originally published on date 2022-01-04T13:15:07.957 and modified on date 2022-01-12T21:20:01.473. The vulnerability is described as A download of code without integrity check vulnerability in the "execute restore src-vis" command of FortiOS before 7.0.3 may allow a local authenticated attacker to download arbitrary files

on the device via specially crafted update packages.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2021-43711 and source identifier nvd@nist.gov was originally published on date 2022-01-04T14:15:08.127 and modified on date 2022-01-12T15:25:43.887. The vulnerability is described as The downloadFlile.cgi binary file in TOTOLINK EX200 V4.0.3c.7646_B20201211 has a command injection vulnerability when receiving GET parameters. The parameter name can be constructed for unauthenticated command execution.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-3842 and source identifier nvd@nist.gov was originally published on date 2022-01-04T15:15:07.833 and modified on date 2022-01-12T21:15:39.057. The vulnerability is described as nltk is vulnerable to Inefficient Regular Expression Complexity. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-45913 and source identifier nvd@nist.gov was originally published on date 2022-01-04T15:15:07.897 and modified on date 2022-01-13T16:47:30.893. The vulnerability is described as A hardcoded key in ControlUp Real-Time Agent (cuAgent.exe) before 8.2.5 may allow a potential attacker to run OS commands via a WCF channel.. It has severity HIGH with exploitability score 8.0 and impact score 10.0.

The CVE with id CVE-2021-45978 and source identifier nvd@nist.gov was originally published on date 2022-01-04T15:15:07.943 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as Foxit PDF Reader and PDF Editor before 11.1 on macOS allow remote attackers to execute arbitrary code via xfa.host.gotoURL in the XFA API.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-45979 and source identifier nvd@nist.gov was originally published on date 2022-01-04T15:15:07.990 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as Foxit PDF Reader and PDF Editor before 11.1 on macOS allow remote attackers to execute arbitrary code via app.launchURL in the JavaScript API.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-45980 and source identifier nvd@nist.gov was originally published on date 2022-01-04T15:15:08.037 and modified on date 2022-01-11T21:13:22.303. The vulnerability is described as Foxit PDF Reader and PDF Editor before 11.1 on macOS allow remote attackers to execute arbitrary code via getURL in the JavaScript API.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-40148 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:09.193 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as In Modem EMM, there is a possible information disclosure due to a missing data encryption. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00716585; Issue ID: ALPS05886933.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-41789 and source identifier nvd@nist.gov was originally published on

date 2022-01-04T16:15:09.527 and modified on date 2022-01-14T16:11:30.903. The vulnerability is described as In wifi driver, there is a possible system crash due to a missing validation check. This could lead to remote denial of service from a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20190426015; Issue ID: GN20190426015.. It has severity MEDIUM with exploitability score 6.5 and impact score 6.9.

The CVE with id CVE-2021-45389 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:09.727 and modified on date 2022-09-01T00:15:08.657. The vulnerability is described as A flaw was found with the JWT token. A self-signed JWT token could be injected into the update manager and bypass the authentication process, thus could escalate privileges. This affects StarWind SAN and NAS build 1578 and StarWind Command Center build 6864.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45912 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:09.953 and modified on date 2022-01-14T19:24:17.197. The vulnerability is described as An unauthenticated Named Pipe channel in Controlup Real-Time Agent (cuAgent.exe) before 8.5 potentially allows an attacker to run OS commands via the ProcessActionRequest WCF method.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2022-20012 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.167 and modified on date 2022-01-11T19:56:36.063. The vulnerability is described as In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2022-20013 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.237 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as In vow driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05837742.. It has severity MEDIUM with exploitability score 3.4 and impact score 6.4.

The CVE with id CVE-2022-20014 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.287 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as In vow driver, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05857308; Issue ID: ALPS05857308.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2022-20015 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.333 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as In kd_camera_hw driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966.. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2022-20016 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.383 and modified on date 2022-01-11T19:38:19.430. The vulnerability is described as In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986.. It has severity MEDIUM with exploitability score 3.9 and impact score 6.4.

The CVE with id CVE-2022-20018 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.440 and modified on date 2022-01-11T20:38:18.310. The vulnerability is described as In seninf driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018.. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2022-20019 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.493 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620.. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2022-20020 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.547 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as In libvcodecdrv, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05943906; Issue ID: ALPS05943906.. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2022-20021 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.600 and modified on date 2022-01-11T19:07:53.067. The vulnerability is described as In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513.. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2022-20022 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.653 and modified on date 2022-01-11T19:13:47.303. The vulnerability is described as In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578.. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2022-20023 and source identifier nvd@nist.gov was originally published on date 2022-01-04T16:15:10.703 and modified on date 2022-01-11T19:17:38.807. The vulnerability is described as In Bluetooth, there is a possible application crash due to bluetooth flooding a device

with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608.. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2021-3845 and source identifier nvd@nist.gov was originally published on date 2022-01-04T17:15:08.230 and modified on date 2022-10-28T19:28:47.393. The vulnerability is described as ws-scrcpy is vulnerable to External Control of File Name or Path. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-39143 and source identifier nvd@nist.gov was originally published on date 2022-01-04T18:15:08.087 and modified on date 2022-01-18T14:45:24.663. The vulnerability is described as Spinnaker is an open source, multi-cloud continuous delivery platform. A path traversal vulnerability was discovered in uses of TAR files by AppEngine for deployments. This uses a utility to extract files locally for deployment without validating the paths in that deployment don't override system files. This would allow an attacker to override files on the container, POTENTIALLY introducing a MITM type attack vector by replacing libraries or injecting wrapper files. Users are advised to update as soon as possible. For users unable to update disable Google AppEngine deployments and/or disable artifacts that provide TARs.. It has severity LOW with exploitability score 3.9 and impact score 4.9.

The CVE with id CVE-2022-0086 and source identifier nvd@nist.gov was originally published on date 2022-01-04T18:15:08.257 and modified on date 2022-01-08T02:44:42.867. The vulnerability is described as uppy is vulnerable to Server-Side Request Forgery (SSRF). It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-24042 and source identifier nvd@nist.gov was originally published on date 2022-01-04T19:15:14.603 and modified on date 2022-01-14T19:37:51.337. The vulnerability is described as The calling logic for WhatsApp for Android prior to v2.21.23, WhatsApp Business for Android prior to v2.21.23, WhatsApp for iOS prior to v2.21.230, WhatsApp Business for iOS prior to v2.21.230, WhatsApp for KaiOS prior to v2.2143, WhatsApp Desktop prior to v2.2146 could have allowed an out-of-bounds write if a user makes a 1:1 call to a malicious actor.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-41141 and source identifier nvd@nist.gov was originally published on date 2022-01-04T19:15:14.687 and modified on date 2022-11-16T19:07:09.427. The vulnerability is described as PJSIP is a free and open source multimedia communication library written in the C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In various parts of PJSIP, when error/failure occurs, it is found that the function returns without releasing the currently held locks. This could result in a system deadlock, which cause a denial of service for the users. No release has yet been made which contains the linked fix commit. All versions up to an including 2.11.1 are affected. Users may need to manually apply the patch.. It has severity HIGH with exploitability score 10.0 and impact score 6.9.

The CVE with id CVE-2021-41236 and source identifier nvd@nist.gov was originally published on date 2022-01-04T19:15:14.763 and modified on date 2022-01-08T02:45:28.930. The vulnerability is described as OroPlatform is a PHP Business Application Platform. In affected versions the email

template preview is vulnerable to XSS payload added to email template content. An attacker must have permission to create or edit an email template. For successful payload, execution the attacked user must preview a vulnerable email template. There are no workarounds that address this vulnerability. Users are advised to upgrade as soon as is possible.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-41610 and source identifier N/A was originally published on date 2022-01-04T20:15:07.497 and modified on date 2022-01-04T20:15:07.497. The vulnerability is described as ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-27339. Reason: This candidate is a reservation duplicate of CVE-2020-27339. Notes: All CVE users should reference CVE-2020-27339 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.. It has severity N/A with exploitability score N/A and impact score N/A.

The CVE with id CVE-2021-43677 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.550 and modified on date 2022-01-08T02:46:00.583. The vulnerability is described as Fluxbb v1.4.12 is affected by a Cross Site Scripting (XSS) vulnerability.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-43832 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.600 and modified on date 2022-01-14T02:12:09.030. The vulnerability is described as Spinnaker is an open source, multi-cloud continuous delivery platform. Spinnaker has improper permissions allowing pipeline creation & execution. This lets an arbitrary user with access to the gate endpoint to create a pipeline and execute it without authentication. If users haven't setup Role-based access control (RBAC) with-in spinnaker, this enables remote execution and access to deploy almost any resources on any account. Patches are available on the latest releases of the supported branches and users are advised to upgrade as soon as possible. Users unable to upgrade should enable RBAC on ALL accounts and applications. This mitigates the ability of a pipeline to affect any accounts. Block application access unless permission are enabled. Users should make sure ALL application creation is restricted via appropriate wildcards.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-43850 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.667 and modified on date 2022-01-14T02:50:53.677. The vulnerability is described as Discourse is an open source platform for community discussion. In affected versions admins users can trigger a Denial of Service attack via the `/message-bus/_diagnostics` path. The impact of this vulnerability is greater on multisite Discourse instances (where multiple forums are served from a single application server) where any admin user on any of the forums are able to visit the `/message-bus/_diagnostics` path. The problem has been patched. Please upgrade to 2.8.0.beta10 or 2.7.12. No workarounds for this issue exist.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-43852 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.730 and modified on date 2022-01-12T21:11:39.990. The vulnerability is described as OroPlatform is a PHP Business Application Platform. In affected versions by sending a specially crafted request, an attacker could inject properties into existing JavaScript language construct prototypes, such as objects. Later this injection may lead to JS code execution by libraries

that are vulnerable to Prototype Pollution. This issue has been patched in version 4.2.8. Users unable to upgrade may configure a firewall to drop requests containing next strings: `__proto__` , `constructor[prototype]`, and `constructor.prototype` to mitigate this issue.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2022-21643 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.797 and modified on date 2022-01-21T14:24:44.283. The vulnerability is described as USOC is an open source CMS with a focus on simplicity. In affected versions USOC allows for SQL injection via register.php. In particular usernames, email addresses, and passwords provided by the user were not sanitized and were used directly to construct a sql statement. Users are advised to upgrade as soon as possible. There are not workarounds for this issue.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2022-21644 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.860 and modified on date 2022-01-21T14:24:50.440. The vulnerability is described as USOC is an open source CMS with a focus on simplicity. In affected versions USOC allows for SQL injection via usersearch.php. In search terms provided by the user were not sanitized and were used directly to construct a sql statement. The only users permitted to search are site admins. Users are advised to upgrade as soon as possible. There are not workarounds for this issue.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2022-21647 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:07.930 and modified on date 2022-01-20T15:04:23.823. The vulnerability is described as CodeIgniter is an open source PHP full-stack web framework. Deserialization of Untrusted Data was found in the `old()` function in CodeIgniter4. Remote attackers may inject auto-loadable arbitrary objects with this vulnerability, and possibly execute existing PHP code on the server. We are aware of a working exploit, which can lead to SQL injection. Users are advised to upgrade to v4.1.6 or later. Users unable to upgrade as advised to not use the `old()` function and form_helper nor `RedirectResponse::withInput()` and `redirect()->withInput()`.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2022-21648 and source identifier nvd@nist.gov was originally published on date 2022-01-04T20:15:08.003 and modified on date 2022-01-13T17:59:35.183. The vulnerability is described as Latte is an open source template engine for PHP. Versions since 2.8.0 Latte has included a template sandbox and in affected versions it has been found that a sandbox escape exists allowing for injection into web pages generated from Latte. This may lead to XSS attacks. The issue is fixed in the versions 2.8.8, 2.9.6 and 2.10.8. Users unable to upgrade should not accept template input from untrusted sources.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-21649 and source identifier nvd@nist.gov was originally published on date 2022-01-04T21:15:07.883 and modified on date 2022-01-08T02:46:40.037. The vulnerability is described as Convos is an open source multi-user chat that runs in a web browser. Characters starting with "https://" in the chat window create an <a> tag. Stored XSS vulnerability using onfocus and autofocus occurs because escaping exists for "<" or ">" but escaping for double quotes does not exist. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible.. It has severity LOW with exploitability score 6.8 and impact

score 2.9.

The CVE with id CVE-2022-21650 and source identifier nvd@nist.gov was originally published on date 2022-01-04T21:15:07.943 and modified on date 2022-01-11T21:48:32.967. The vulnerability is described as Convos is an open source multi-user chat that runs in a web browser. You can't use SVG extension in Convos' chat window, but you can upload a file with an .html extension. By uploading an SVG file with an html extension the upload filter can be bypassed. This causes Stored XSS. Also, after uploading a file the XSS attack is triggered upon a user viewing the file. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-22045 and source identifier nvd@nist.gov was originally published on date 2022-01-04T22:15:07.467 and modified on date 2022-01-27T17:40:20.980. The vulnerability is described as VMware ESXi (7.0, 6.7 before ESXi670-202111101-SG and 6.5 before ESXi650-202110101-SG), VMware Workstation (16.2.0) and VMware Fusion (12.2.0) contains a heap-overflow vulnerability in CD-ROM device emulation. A malicious actor with access to a virtual machine with CD-ROM device emulation may be able to exploit this vulnerability in conjunction with other issues to execute code on the hypervisor from a virtual machine.. It has severity MEDIUM with exploitability score 3.4 and impact score 10.0.

The CVE with id CVE-2021-41388 and source identifier nvd@nist.gov was originally published on date 2022-01-04T22:15:07.527 and modified on date 2022-01-13T17:15:10.267. The vulnerability is described as Netskope client prior to 89.x on macOS is impacted by a local privilege escalation vulnerability. The XPC implementation of nsAuxiliarySvc process does not perform validation on new connections before accepting the connection. Thus any low privileged user can connect and call external methods defined in XPC service as root, elevating their privilege to the highest level.. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-45115 and source identifier nvd@nist.gov was originally published on date 2022-01-05T00:15:07.907 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as An issue was discovered in Django 2.2 before 2.2.26, 3.2 before 3.2.11, and 4.0 before 4.0.1. UserAttributeSimilarityValidator incurred significant overhead in evaluating a submitted password that was artificially large in relation to the comparison values. In a situation where access to user registration was unrestricted, this provided a potential vector for a denial-of-service attack.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-45116 and source identifier nvd@nist.gov was originally published on date 2022-01-05T00:15:07.953 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as An issue was discovered in Django 2.2 before 2.2.26, 3.2 before 3.2.11, and 4.0 before 4.0.1. Due to leveraging the Django Template Language's variable resolution logic, the dictsort template filter was potentially vulnerable to information disclosure, or an unintended method call, if passed a suitably crafted key.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-45452 and source identifier nvd@nist.gov was originally published on date 2022-01-05T00:15:07.997 and modified on date 2022-02-11T05:30:24.907. The vulnerability is described as Storage.save in Django 2.2 before 2.2.26, 3.2 before 3.2.11, and 4.0 before 4.0.1

allows directory traversal if crafted filenames are directly passed to it.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-43946 and source identifier nvd@nist.gov was originally published on date 2022-01-05T04:15:07.497 and modified on date 2023-02-24T14:11:14.347. The vulnerability is described as Affected versions of Atlassian Jira Server and Data Center allow authenticated remote attackers to add administrator groups to filter subscriptions via a Broken Access Control vulnerability in the /secure/EditSubscription.jspa endpoint. The affected versions are before version 8.13.21, and from version 8.14.0 before 8.20.9.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-22567 and source identifier nvd@nist.gov was originally published on date 2022-01-05T11:15:08.120 and modified on date 2022-01-12T18:43:51.137. The vulnerability is described as Bidirectional Unicode text can be interpreted and compiled differently than how it appears in editors which can be exploited to get nefarious code passed a code review by appearing benign. An attacker could embed a source that is invisible to a code reviewer that modifies the behavior of a program in unexpected ways.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2020-15933 and source identifier nvd@nist.gov was originally published on date 2022-01-05T12:15:07.977 and modified on date 2022-01-12T20:03:45.657. The vulnerability is described as A exposure of sensitive information to an unauthorized actor in Fortinet FortiMail versions 6.0.9 and below, FortiMail versions 6.2.4 and below FortiMail versions 6.4.1 and 6.4.0 allows attacker to obtain potentially sensitive software-version information via client-side resources inspection.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-31589 and source identifier nvd@nist.gov was originally published on date 2022-01-05T12:15:08.063 and modified on date 2022-02-07T18:59:56.610. The vulnerability is described as A cross-site scripting (XSS) vulnerability has been reported and confirmed for BeyondTrust Secure Remote Access Base Software version 6.0.1 and older, which allows the injection of unauthenticated, specially-crafted web requests without proper sanitization.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-41043 and source identifier nvd@nist.gov was originally published on date 2022-01-05T12:15:08.127 and modified on date 2022-01-12T20:28:09.127. The vulnerability is described as Use after free in tcpslice triggers AddressSanitizer, no other confirmed impact.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-22107 and source identifier nvd@nist.gov was originally published on date 2022-01-05T15:15:07.720 and modified on date 2022-01-08T02:49:40.197. The vulnerability is described as In Daybyday CRM, versions 2.0.0 through 2.2.0 are vulnerable to Missing Authorization. An attacker that has the lowest privileges account (employee type user), can view the appointments of all users in the system including administrators. However, this type of user is not authorized to view the calendar at all.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2022-22108 and source identifier nvd@nist.gov was originally published on

date 2022-01-05T15:15:07.787 and modified on date 2022-01-08T02:49:50.347. The vulnerability is described as In Daybyday CRM, versions 2.0.0 through 2.2.0 are vulnerable to Missing Authorization. An attacker that has the lowest privileges account (employee type user), can view the absences of all users in the system including administrators. This type of user is not authorized to view this kind of information.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2022-22109 and source identifier nvd@nist.gov was originally published on date 2022-01-05T15:15:07.857 and modified on date 2022-01-08T02:50:02.153. The vulnerability is described as In Daybyday CRM, version 2.2.0 is vulnerable to Stored Cross-Site Scripting (XSS) vulnerability that allows low privileged application users to store malicious scripts in the title field of new tasks. These scripts are executed in a victim’s browser when they open the “/tasks” page to view all the tasks.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2022-22110 and source identifier nvd@nist.gov was originally published on date 2022-01-05T15:15:07.923 and modified on date 2022-01-21T14:24:35.657. The vulnerability is described as In Daybyday CRM, versions 1.1 through 2.2.0 enforce weak password requirements in the user update functionality. A user with privileges to update his password could change it to a weak password, such as those with a length of a single character. This may allow an attacker to brute-force users’ passwords with minimal to no computational effort.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2022-22111 and source identifier nvd@nist.gov was originally published on date 2022-01-05T15:15:07.990 and modified on date 2022-01-08T02:51:33.377. The vulnerability is described as In DayByDay CRM, version 2.2.0 is vulnerable to missing authorization. Any application user in the application who has update user permission enabled is able to change the password of other users, including the administrator’s. This allows the attacker to gain access to the highest privileged user in the application.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-28711 and source identifier nvd@nist.gov was originally published on date 2022-01-05T17:15:09.017 and modified on date 2022-04-06T16:18:34.433. The vulnerability is described as Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-28712 and source identifier nvd@nist.gov was originally published on date 2022-01-05T17:15:09.070 and modified on date 2022-04-06T16:33:36.737. The vulnerability is described as Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities

correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-28713 and source identifier nvd@nist.gov was originally published on date 2022-01-05T17:15:09.120 and modified on date 2022-04-06T16:35:54.087. The vulnerability is described as Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-38918 and source identifier nvd@nist.gov was originally published on date 2022-01-05T17:15:09.190 and modified on date 2022-01-12T18:45:31.570. The vulnerability is described as IBM PowerVM Hypervisor FW860, FW940, FW950, and FW1010, through a specific sequence of VM management operations could lead to a violation of the isolation between peer VMs. IBM X-Force ID: 210019.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-43779 and source identifier nvd@nist.gov was originally published on date 2022-01-05T19:15:08.627 and modified on date 2022-08-09T00:52:26.057. The vulnerability is described as GLPI is an open source IT Asset Management, issue tracking system and service desk system. The GLPI addressing plugin in versions < 2.9.1 suffers from authenticated Remote Code Execution vulnerability, allowing access to the server's underlying operating system using command injection abuse of functionality. There is no workaround for this issue and users are advised to upgrade or to disable the addressing plugin.. It has severity HIGH with exploitability score 8.0 and impact score 10.0.

The CVE with id CVE-2021-43816 and source identifier nvd@nist.gov was originally published on date 2022-01-05T19:15:08.717 and modified on date 2022-04-01T14:50:57.473. The vulnerability is described as containerd is an open source container runtime. On installations using SELinux, such as EL8 (CentOS, RHEL), Fedora, or SUSE MicroOS, with containerd since v1.5.0-beta.0 as the backing container runtime interface (CRI), an unprivileged pod scheduled to the node may bind mount, via hostPath volume, any privileged, regular file on disk for complete read/write access (sans delete). Such is achieved by placing the in-container location of the hostPath volume mount at either `/etc/hosts`, `/etc/hostname`, or `/etc/resolv.conf`. These locations are being relabeled indiscriminately to match the container process-label which effectively elevates permissions for

savvy containers that would not normally be able to access privileged host files. This issue has been resolved in version 1.5.9. Users are advised to upgrade as soon as possible.. It has severity MEDIUM with exploitability score 6.8 and impact score 6.4.

The CVE with id CVE-2022-21642 and source identifier nvd@nist.gov was originally published on date 2022-01-05T19:15:09.053 and modified on date 2022-01-12T20:17:45.500. The vulnerability is described as Discourse is an open source platform for community discussion. In affected versions when composing a message from topic the composer user suggestions reveals whisper participants. The issue has been patched in stable version 2.7.13 and beta version 2.8.0.beta11. There is no workaround for this issue and users are advised to upgrade.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-45830 and source identifier nvd@nist.gov was originally published on date 2022-01-05T20:15:07.897 and modified on date 2022-01-12T20:15:39.667. The vulnerability is described as A heap-based buffer overflow vulnerability exists in HDF5 1.13.1-1 via H5F_addr_decode_len in /hdf5/src/H5Fint.c, which could cause a Denial of Service.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45831 and source identifier nvd@nist.gov was originally published on date 2022-01-05T20:15:07.950 and modified on date 2023-05-27T04:15:18.997. The vulnerability is described as A Null Pointer Dereference vulnerability exitgs in GPAC 1.0.1 in MP4Box via __strlen_avx2, which causes a Denial of Service.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-21651 and source identifier nvd@nist.gov was originally published on date 2022-01-05T20:15:08.020 and modified on date 2022-01-12T18:43:22.343. The vulnerability is described as Shopware is an open source e-commerce software platform. An open redirect vulnerability has been discovered. Users may be arbitrary redirected due to incomplete URL handling in the shopware router. This issue has been resolved in version 5.7.7. There is no workaround and users are advised to upgrade as soon as possible.. It has severity MEDIUM with exploitability score 8.6 and impact score 4.9.

The CVE with id CVE-2022-21652 and source identifier nvd@nist.gov was originally published on date 2022-01-05T20:15:08.117 and modified on date 2022-01-12T18:28:21.877. The vulnerability is described as Shopware is an open source e-commerce software platform. In affected versions shopware would not invalidate a user session in the event of a password change. With version 5.7.7 the session validation was adjusted, so that sessions created prior to the latest password change of a customer account can't be used to login with said account. This also means, that upon a password change, all existing sessions for a given customer account are automatically considered invalid. There is no workaround for this issue.. It has severity MEDIUM with exploitability score 8.0 and impact score 4.9.

The CVE with id CVE-2021-45832 and source identifier nvd@nist.gov was originally published on date 2022-01-05T21:15:07.780 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as A Stack-based Buffer Overflow Vulnerability exists in HDF5 1.13.1-1 at at hdf5/src/H5Eint.c, which causes a Denial of Service (context-dependent).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-45833 and source identifier nvd@nist.gov was originally published on date 2022-01-05T21:15:07.833 and modified on date 2022-01-12T17:42:20.760. The vulnerability is described as A Stack-based Buffer Overflow Vulnerability exists in HDF5 1.13.1-1 via the H5D__create_chunk_file_map_hyper function in /hdf5/src/H5Dchunk.c, which causes a Denial of Service (context-dependent).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-21653 and source identifier nvd@nist.gov was originally published on date 2022-01-05T21:15:07.890 and modified on date 2022-01-12T18:54:46.157. The vulnerability is described as Jawn is an open source JSON parser. Extenders of the `org.typelevel.jawn.SimpleFacade` and `org.typelevel.jawn.MutableFacade` who don't override `objectContext()` are vulnerable to a hash collision attack which may result in a denial of service. Most applications do not implement these traits directly, but inherit from a library. `jawn-parser-1.3.1` fixes this issue and users are advised to upgrade. For users unable to upgrade override `objectContext()` to use a collision-safe collection.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2020-5956 and source identifier nvd@nist.gov was originally published on date 2022-01-05T23:15:07.920 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as An issue was discovered in SdLegacySmm in Insyde InsydeH2O with kernel 5.1 before 05.15.11, 5.2 before 05.25.11, 5.3 before 05.34.11, and 5.4 before 05.42.11. The software SMI handler allows untrusted external input because it does not verify CommBuffer.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-45969 and source identifier nvd@nist.gov was originally published on date 2022-01-05T23:15:08.833 and modified on date 2022-03-29T16:35:03.667. The vulnerability is described as An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the CommBuffer+8 location).. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-45970 and source identifier nvd@nist.gov was originally published on date 2022-01-05T23:15:08.887 and modified on date 2022-03-29T16:35:09.413. The vulnerability is described as An issue was discovered in IdeBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the status code saved at the CommBuffer+4 location).. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-46038 and source identifier nvd@nist.gov was originally published on date 2022-01-05T23:15:08.947 and modified on date 2023-05-27T04:15:19.083. The vulnerability is described as A Pointer Dereference vulnerability exists in GPAC 1.0.1 in unlink_chunk.isra, which causes a Denial of Service (context-dependent).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2020-23986 and source identifier nvd@nist.gov was originally published on date 2022-01-06T00:15:07.737 and modified on date 2022-01-08T02:53:16.533. The vulnerability is described as Github Read Me Stats commit 3c7220e4f7144f6cb068fd433c774f6db47ccb95 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the function renderError.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2020-27428 and source identifier nvd@nist.gov was originally published on date 2022-01-06T00:15:07.790 and modified on date 2022-01-12T17:17:56.067. The vulnerability is described as A DOM-based cross-site scripting (XSS) vulnerability in Scratch-Svg-Renderer v0.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted sb3 file.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-41842 and source identifier nvd@nist.gov was originally published on date 2022-01-06T00:15:07.860 and modified on date 2022-03-01T19:58:48.343. The vulnerability is described as An issue was discovered in AtaLegacySmm in the kernel 5.0 before 05.08.46, 5.1 before 05.16.46, 5.2 before 05.26.46, 5.3 before 05.35.46, 5.4 before 05.43.46, and 5.5 before 05.51.45 in Insyde InsydeH2O. Code execution can occur because the SMI handler lacks a CommBuffer check.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45971 and source identifier nvd@nist.gov was originally published on date 2022-01-06T00:15:07.910 and modified on date 2022-03-29T16:35:15.030. The vulnerability is described as An issue was discovered in SdHostDriver in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (CommBufferData).. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-43947 and source identifier nvd@nist.gov was originally published on date 2022-01-06T01:15:07.917 and modified on date 2022-03-30T13:29:49.470. The vulnerability is described as Affected versions of Atlassian Jira Server and Data Center allow remote attackers with administrator privileges to execute arbitrary code via a Remote Code Execution (RCE) vulnerability in the Email Templates feature. This issue bypasses the fix of https://jira.atlassian.com/browse/JSDSERVER-8665. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.. It has severity HIGH with exploitability score 8.0 and impact score 10.0.

The CVE with id CVE-2022-0121 and source identifier nvd@nist.gov was originally published on date 2022-01-06T03:15:06.790 and modified on date 2023-08-02T09:15:10.317. The vulnerability is described as Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hoppscotch hoppscotch/hoppscotch.This issue affects hoppscotch/hoppscotch before 2.1.1.

. It has severity MEDIUM with exploitability score 6.8 and impact score 6.4.

The CVE with id CVE-2021-46141 and source identifier nvd@nist.gov was originally published on date 2022-01-06T04:15:06.917 and modified on date 2022-02-05T02:35:38.710. The vulnerability is described as An issue was discovered in uriparser before 0.9.6. It performs invalid free operations in

uriFreeUriMembers and uriMakeOwner.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46142 and source identifier nvd@nist.gov was originally published on date 2022-01-06T04:15:06.967 and modified on date 2022-02-05T02:36:15.083. The vulnerability is described as An issue was discovered in uriparser before 0.9.6. It performs invalid free operations in uriNormalizeSyntax.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46143 and source identifier nvd@nist.gov was originally published on date 2022-01-06T04:15:07.017 and modified on date 2022-10-06T19:11:54.880. The vulnerability is described as In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-46144 and source identifier nvd@nist.gov was originally published on date 2022-01-06T05:15:09.420 and modified on date 2022-04-01T15:21:04.253. The vulnerability is described as Roundcube before 1.4.13 and 1.5.x before 1.5.2 allows XSS via an HTML e-mail message with crafted Cascading Style Sheets (CSS) token sequences.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-0122 and source identifier nvd@nist.gov was originally published on date 2022-01-06T05:15:09.490 and modified on date 2022-01-12T20:14:22.237. The vulnerability is described as forge is vulnerable to URL Redirection to Untrusted Site. It has severity MEDIUM with exploitability score 8.6 and impact score 4.9.

The CVE with id CVE-2022-22704 and source identifier nvd@nist.gov was originally published on date 2022-01-06T05:15:09.580 and modified on date 2023-08-08T14:21:49.707. The vulnerability is described as The zabbix-agent2 package before 5.4.9-r1 for Alpine Linux sometimes allows privilege escalation to root because the design incorrectly expected that systemd would (in effect) determine part of the configuration.. It has severity HIGH with exploitability score 10.0 and impact score 10.0.

The CVE with id CVE-2021-46145 and source identifier nvd@nist.gov was originally published on date 2022-01-06T06:15:07.137 and modified on date 2022-01-18T17:43:12.923. The vulnerability is described as The keyfob subsystem in Honda Civic 2012 vehicles allows a replay attack for unlocking. This is related to a non-expiring rolling code and counter resynchronization.. It has severity LOW with exploitability score 5.5 and impact score 2.9.

The CVE with id CVE-2022-22707 and source identifier nvd@nist.gov was originally published on date 2022-01-06T06:15:07.243 and modified on date 2022-01-13T20:52:29.263. The vulnerability is described as In lighttpd 1.4.46 through 1.4.63, the mod_extforward_Forwarded function of the mod_extforward plugin has a stack-based buffer overflow (4 bytes representing -1), as demonstrated by remote denial of service (daemon crash) in a non-default configuration. The non-default configuration requires handling of the Forwarded header in a somewhat unusual manner. Also, a 32-bit system is much more likely to be affected than a 64-bit system.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-36737 and source identifier nvd@nist.gov was originally published on date 2022-01-06T09:15:07.117 and modified on date 2022-01-12T20:24:30.767. The vulnerability is

described as The input fields of the Apache Pluto UrlTestPortlet are vulnerable to Cross-Site Scripting (XSS) attacks. Users should migrate to version 3.1.1 of the v3-demo-portlet.war artifact. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-36738 and source identifier nvd@nist.gov was originally published on date 2022-01-06T09:15:07.273 and modified on date 2022-01-12T15:04:02.023. The vulnerability is described as The input fields in the JSP version of the Apache Pluto Applicant MVCBean CDI portlet are vulnerable to Cross-Site Scripting (XSS) attacks. Users should migrate to version 3.1.1 of the applicant-mvcbean-cdi-jsp-portlet.war artifact. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-36739 and source identifier nvd@nist.gov was originally published on date 2022-01-06T09:15:07.327 and modified on date 2022-01-12T14:51:21.543. The vulnerability is described as The "first name" and "last name" fields of the Apache Pluto 3.1.0 MVCBean JSP portlet maven archetype are vulnerable to Cross-Site Scripting (XSS) attacks.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-44351 and source identifier nvd@nist.gov was originally published on date 2022-01-06T12:15:08.087 and modified on date 2022-01-12T20:48:13.440. The vulnerability is described as An arbitrary file read vulnerability exists in NavigateCMS 2.9 via /navigate/navigate_download.php id parameter.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-44564 and source identifier nvd@nist.gov was originally published on date 2022-01-06T12:15:08.190 and modified on date 2022-01-14T16:46:31.343. The vulnerability is described as A security vulnerability originally reported in the SYNC2101 product, and applicable to specific sub-families of SYNC devices, allows an attacker to download the configuration file used in the device and apply a modified configuration file back to the device. The attack requires network access to the SYNC device and knowledge of its IP address. The attack exploits the unsecured communication channel used between the administration tool Easyconnect and the SYNC device (in the affected family of SYNC products).. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-27738 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:07.967 and modified on date 2022-01-13T18:04:21.017. The vulnerability is described as All request mappings in `StreamingCoordinatorController.java` handling `/kylin/api/streaming_coordinator/*` REST API endpoints did not include any security checks, which allowed an unauthenticated user to issue arbitrary requests, such as assigning/unassigning of streaming cubes, creation/modification and deletion of replica sets, to the Kylin Coordinator. For endpoints accepting node details in HTTP message body, unauthenticated (but limited) server-side request forgery (SSRF) can be achieved. This issue affects Apache Kylin Apache Kylin 3 versions prior to 3.1.2.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-31522 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.027 and modified on date 2022-01-12T20:52:49.923. The vulnerability is described as Kylin can receive user input and load any class through Class.forName(...). This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior

versions; Apache Kylin 4 version 4.0.0 and prior versions.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-36774 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.080 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as Apache Kylin allows users to read data from other database systems using JDBC. The MySQL JDBC driver supports certain properties, which, if left unmitigated, can allow an attacker to execute arbitrary code from a hacker-controlled malicious MySQL server within Kylin server processes. This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-44584 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.133 and modified on date 2022-01-12T14:50:23.647. The vulnerability is described as Cross-site scripting (XSS) vulnerability in index.php in emlog version <= pro-1.0.7 allows remote attackers to inject arbitrary web script or HTML via the s parameter.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-44878 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.180 and modified on date 2022-05-13T15:51:59.780. The vulnerability is described as If an OpenID Connect provider supports the "none" algorithm (i.e., tokens with no signature), pac4j v5.3.0 (and prior) does not refuse it without an explicit configuration on its side or for the "idtoken" response type which is not secure and violates the OpenID Core Specification. The "none" algorithm does not require any signature verification when validating the ID tokens, which allows the attacker to bypass the token validation by injecting a malformed ID token using "none" as the value of "alg" key in the header with an empty signature value.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-45456 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.227 and modified on date 2022-01-13T18:50:42.417. The vulnerability is described as Apache kylin checks the legitimacy of the project before executing some commands with the project name passed in by the user. There is a mismatch between what is being checked and what is being used as the shell command argument in DiagnosisService. This may cause an illegal project name to pass the check and perform the following steps, resulting in a command injection vulnerability. This issue affects Apache Kylin 4.0.0.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-45457 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.283 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as In Apache Kylin, Cross-origin requests with credentials are allowed to be sent from any origin. This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions; Apache Kylin 4 version 4.0.0 and prior versions.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-45458 and source identifier nvd@nist.gov was originally published on date 2022-01-06T13:15:08.330 and modified on date 2023-07-21T16:52:45.507. The vulnerability is described as Apache Kylin provides encryption classes PasswordPlaceholderConfigurer to help

users encrypt their passwords. In the encryption algorithm used by this encryption class, the cipher is initialized with a hardcoded key and IV. If users use class PasswordPlaceholderConfigurer to encrypt their password and configure it into kylin's configuration file, there is a risk that the password may be decrypted. This issue affects Apache Kylin 2 version 2.6.6 and prior versions; Apache Kylin 3 version 3.1.2 and prior versions; Apache Kylin 4 version 4.0.0 and prior versions.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-44590 and source identifier nvd@nist.gov was originally published on date 2022-01-06T14:15:07.867 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as In libming 0.4.8, a memory exhaustion vulnerability exist in the function cws2fws in util/main.c. Remote attackers could launch denial of service attacks by submitting a crafted SWF file that exploits this vulnerability.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-44591 and source identifier nvd@nist.gov was originally published on date 2022-01-06T14:15:07.917 and modified on date 2022-01-13T12:52:33.847. The vulnerability is described as In libming 0.4.8, the parseSWF_DEFINELOSSLESS2 function in util/parser.c lacks a boundary check that would lead to denial-of-service attacks via a crafted SWF file.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46076 and source identifier nvd@nist.gov was originally published on date 2022-01-06T15:15:08.693 and modified on date 2022-01-12T20:27:05.493. The vulnerability is described as Sourcecodester Vehicle Service Management System 1.0 is vulnerable to File upload. An attacker can upload a malicious php file in multiple endpoints it leading to Code Execution.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-46080 and source identifier nvd@nist.gov was originally published on date 2022-01-06T15:15:08.743 and modified on date 2022-01-13T13:53:22.243. The vulnerability is described as A Cross Site Request Forgery (CSRF) vulnerability exists in Vehicle Service Management System 1.0. An successful CSRF attacks leads to Stored Cross Site Scripting Vulnerability.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-45744 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.527 and modified on date 2022-01-07T19:58:08.023. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in bludit 3.13.1 via the TAGS section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-45745 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.570 and modified on date 2022-01-07T19:58:42.870. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Bludit 3.13.1 via the About Plugin in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46067 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.617 and modified on date 2022-01-13T13:03:37.823. The vulnerability is described as In Vehicle Service Management System 1.0 an attacker can steal the cookies leading to Full Account Takeover.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-46068 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.660 and modified on date 2022-01-07T20:02:48.723. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the My Account Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46069 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.707 and modified on date 2022-01-07T20:03:27.280. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Mechanic List Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46070 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.753 and modified on date 2022-01-07T20:03:55.837. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Service Requests Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46071 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.797 and modified on date 2022-01-10T18:17:54.537. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Category List Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46072 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.847 and modified on date 2022-01-07T20:06:59.957. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Vehicle Service Management System 1.0 via the Service List Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46073 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.893 and modified on date 2022-01-11T21:23:01.560. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Vehicle Service Management System 1.0 via the User List Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46074 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.940 and modified on date 2022-01-11T21:27:22.940. The vulnerability is described as A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Vehicle Service Management System 1.0 via the Settings Section in login panel.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46075 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:08.987 and modified on date 2022-07-12T17:42:04.277. The vulnerability is described as A Privilege Escalation vulnerability exists in Sourcecodester Vehicle Service Management System 1.0. Staff account users can access the admin resources and perform CRUD Operations.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-46078 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:09.033 and modified on date 2022-01-13T13:49:48.997. The vulnerability is described as An Unrestricted File Upload vulnerability exists in Sourcecodester Vehicle Service Management System 1.0. A remote attacker can upload malicious files leading to a Stored Cross-Site Scripting vulnerability.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-46079 and source identifier nvd@nist.gov was originally published on date 2022-01-06T16:15:09.080 and modified on date 2022-01-12T18:06:25.070. The vulnerability is described as An Unrestricted File Upload vulnerability exists in Sourcecodester Vehicle Service Management System 1.0. A remote attacker can upload malicious files leading to Html Injection.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2022-0128 and source identifier nvd@nist.gov was originally published on date 2022-01-06T17:15:07.883 and modified on date 2022-11-02T13:18:35.983. The vulnerability is described as vim is vulnerable to Out-of-bounds Read. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-28714 and source identifier nvd@nist.gov was originally published on date 2022-01-06T18:15:07.760 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as Guest can force Linux netback driver to hog large amounts of kernel memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714). It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-28715 and source identifier nvd@nist.gov was originally published on date 2022-01-06T18:15:07.813 and modified on date 2023-08-08T14:22:24.967. The vulnerability is described as Guest can force Linux netback driver to hog large amounts of kernel memory T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714). It has severity LOW with exploitability score 3.9 and impact

score 2.9.

The CVE with id CVE-2021-43045 and source identifier nvd@nist.gov was originally published on date 2022-01-06T18:15:07.863 and modified on date 2022-01-14T01:08:05.953. The vulnerability is described as A vulnerability in the .NET SDK of Apache Avro allows an attacker to allocate excessive resources, potentially causing a denial-of-service attack. This issue affects .NET applications using Apache Avro version 1.10.2 and prior versions. Users should update to version 1.11.0 which addresses this issue.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-4194 and source identifier nvd@nist.gov was originally published on date 2022-01-06T18:15:07.920 and modified on date 2022-07-25T10:24:25.243. The vulnerability is described as bookstack is vulnerable to Improper Access Control. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-46039 and source identifier nvd@nist.gov was originally published on date 2022-01-06T20:15:08.657 and modified on date 2023-05-27T04:15:19.153. The vulnerability is described as A Pointer Dereference Vulnerabilty exists in GPAC 1.0.1 via the shift_chunk_offsets.part function, which causes a Denial of Service (context-dependent).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46040 and source identifier nvd@nist.gov was originally published on date 2022-01-06T20:15:08.723 and modified on date 2023-05-27T04:15:19.233. The vulnerability is described as A Pointer Dereference Vulnerabilty exists in GPAC 1.0.1 via the finplace_shift_moov_meta_offsets function, which causes a Denial of Servie (context-dependent).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46041 and source identifier nvd@nist.gov was originally published on date 2022-01-06T20:15:08.777 and modified on date 2023-05-27T04:15:19.317. The vulnerability is described as A Segmentation Fault Vulnerability exists in GPAC 1.0.1 via the co64_box_new function, which causes a Denial of Service.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46042 and source identifier nvd@nist.gov was originally published on date 2022-01-06T20:15:08.843 and modified on date 2023-05-27T04:15:19.390. The vulnerability is described as A Pointer Dereference Vulnerability exists in GPAC 1.0.1 via the _fseeko function, which causes a Denial of Service.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-42841 and source identifier nvd@nist.gov was originally published on date 2022-01-06T21:15:08.080 and modified on date 2022-01-11T16:47:17.833. The vulnerability is described as Insta HMS before 12.4.10 is vulnerable to XSS because of improper validation of user-supplied input by multiple scripts. A remote attacker could exploit this vulnerability via a crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46043 and source identifier nvd@nist.gov was originally published on date 2022-01-06T21:15:08.130 and modified on date 2023-05-27T04:15:19.470. The vulnerability is described as A Pointer Dereference Vulnerability exits in GPAC 1.0.1 in the gf_list_count function, which causes a Denial of Service.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-46044 and source identifier nvd@nist.gov was originally published on date 2022-01-06T21:15:08.177 and modified on date 2023-05-27T04:15:19.547. The vulnerability is described as A Pointer Dereference Vulnerabilty exists in GPAC 1.0.1via ShiftMetaOffset.isra, which causes a Denial of Service (context-dependent).. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2022-21661 and source identifier nvd@nist.gov was originally published on date 2022-01-06T23:15:07.933 and modified on date 2022-04-12T18:47:13.057. The vulnerability is described as WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain way. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this vulnerability.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2022-21662 and source identifier nvd@nist.gov was originally published on date 2022-01-06T23:15:08.003 and modified on date 2022-04-12T18:48:50.120. The vulnerability is described as WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Low-privileged authenticated users (like author) in WordPress core are able to execute JavaScript/perform stored XSS attack, which can affect high-privileged users. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2022-21663 and source identifier nvd@nist.gov was originally published on date 2022-01-06T23:15:08.067 and modified on date 2023-06-27T19:03:59.090. The vulnerability is described as WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2022-21664 and source identifier nvd@nist.gov was originally published on date 2022-01-06T23:15:08.130 and modified on date 2022-04-12T18:53:08.027. The vulnerability is described as WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's

potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-25743 and source identifier nvd@nist.gov was originally published on date 2022-01-07T00:15:07.817 and modified on date 2022-02-28T15:22:21.580. The vulnerability is described as kubectl does not neutralize escape, meta or control sequences contained in the raw data it outputs to a terminal. This includes but is not limited to the unstructured string fields in objects such as Events.. It has severity LOW with exploitability score 3.9 and impact score 2.9.

The CVE with id CVE-2021-38674 and source identifier nvd@nist.gov was originally published on date 2022-01-07T02:15:07.143 and modified on date 2022-01-14T19:57:13.040. The vulnerability is described as A cross-site scripting (XSS) vulnerability has been reported to affect QTS, QuTS hero and QuTScloud. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of QTS, QuTS hero and QuTScloud: QuTS hero h4.5.4.1771 build 20210825 and later QTS 4.5.4.1787 build 20210910 and later QuTScloud c4.5.7.1864 and later. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2020-10137 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:15.817 and modified on date 2022-01-18T17:12:45.303. The vulnerability is described as Z-Wave devices based on Silicon Labs 700 series chipsets using S2 do not adequately authenticate or encrypt FIND_NODE_IN_RANGE frames, allowing a remote, unauthenticated attacker to inject a FIND_NODE_IN_RANGE frame with an invalid random payload, denying service by blocking the processing of upcoming events.. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2020-29050 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.077 and modified on date 2022-04-01T15:19:14.987. The vulnerability is described as SphinxSearch in Sphinx Technologies Sphinx through 3.1.1 allows directory traversal (in conjunction with CVE-2019-14511) because the mysql client can be used for CALL SNIPPETS and load_file operations on a full pathname (e.g., a file in the /etc directory). NOTE: this is unrelated to CMUSphinx.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2020-9057 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.150 and modified on date 2022-01-18T17:10:27.780. The vulnerability is described as Z-Wave devices based on Silicon Labs 100, 200, and 300 series chipsets do not support encryption, allowing an attacker within radio range to take control of or cause a denial of service to a vulnerable device. An attacker can also capture and replay Z-Wave traffic. Firmware upgrades cannot directly address this vulnerability as it is an issue with the Z-Wave specification for these legacy chipsets. One way to protect against this vulnerability is to use 500 or 700 series chipsets that support Security 2 (S2) encryption. As examples, the Linear WADWAZ-1 version 3.43 and WAPIRZ-1 version 3.43 (with 300 series chipsets) are vulnerable.. It has severity HIGH with exploitability score 6.5 and impact score 10.0.

The CVE with id CVE-2020-9058 and source identifier nvd@nist.gov was originally published on

date 2022-01-10T14:10:16.227 and modified on date 2022-01-18T17:09:05.987. The vulnerability is described as Z-Wave devices based on Silicon Labs 500 series chipsets using CRC-16 encapsulation, including but likely not limited to the Linear LB60Z-1 version 3.5, Dome DM501 version 4.26, and Jasco ZW4201 version 4.05, do not implement encryption or replay protection.. It has severity MEDIUM with exploitability score 6.5 and impact score 4.9.

The CVE with id CVE-2020-9059 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.303 and modified on date 2022-09-20T17:16:54.653. The vulnerability is described as Z-Wave devices based on Silicon Labs 500 series chipsets using S0 authentication are susceptible to uncontrolled resource consumption leading to battery exhaustion. As an example, the Schlage BE468 version 3.42 door lock is vulnerable and fails open at a low battery level.. It has severity MEDIUM with exploitability score 6.5 and impact score 6.9.

The CVE with id CVE-2020-9060 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.380 and modified on date 2022-09-20T17:16:46.377. The vulnerability is described as Z-Wave devices based on Silicon Labs 500 series chipsets using S2, including but likely not limited to the ZooZ ZST10 version 6.04, ZooZ ZEN20 version 5.03, ZooZ ZEN25 version 5.03, Aeon Labs ZW090-A version 3.95, and Fibaro FGWPB-111 version 4.3, are susceptible to denial of service and resource exhaustion via malformed SECURITY NONCE GET, SECURITY NONCE GET 2, NO OPERATION, or NIF REQUEST messages.. It has severity MEDIUM with exploitability score 6.5 and impact score 6.9.

The CVE with id CVE-2020-9061 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.463 and modified on date 2022-01-18T17:27:05.997. The vulnerability is described as Z-Wave devices using Silicon Labs 500 and 700 series chipsets, including but not likely limited to the SiLabs UZB-7 version 7.00, ZooZ ZST10 version 6.04, Aeon Labs ZW090-A version 3.95, and Samsung STH-ETH-200 version 6.04, are susceptible to denial of service via malformed routing messages.. It has severity LOW with exploitability score 6.5 and impact score 2.9.

The CVE with id CVE-2021-20046 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.537 and modified on date 2022-01-19T13:44:06.637. The vulnerability is described as A Stack-based buffer overflow in the SonicOS HTTP Content-Length response header allows a remote authenticated attacker to cause Denial of Service (DoS) and potentially results in code execution in the firewall. This vulnerability affected SonicOS Gen 5, Gen 6 and Gen 7 firmware versions.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-20048 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.610 and modified on date 2022-01-19T13:49:53.617. The vulnerability is described as A Stack-based buffer overflow in the SonicOS SessionID HTTP response header allows a remote authenticated attacker to cause Denial of Service (DoS) and potentially results in code execution in the firewall. This vulnerability affected SonicOS Gen 5, Gen 6 and Gen 7 firmware versions.. It has severity MEDIUM with exploitability score 8.0 and impact score 6.4.

The CVE with id CVE-2021-22060 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.680 and modified on date 2022-05-13T15:52:15.253. The vulnerability is described as In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log

entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-22569 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.747 and modified on date 2023-04-18T09:15:07.203. The vulnerability is described as An issue in protobuf-java allowed the interleaving of com.google.protobuf.UnknownFieldSet fields in such a way that would be processed out of order. A small malicious payload can occupy the parser for several minutes by creating large numbers of short-lived objects that cause frequent, repeated pauses. We recommend upgrading libraries beyond the vulnerable versions.. It has severity MEDIUM with exploitability score 8.6 and impact score 2.9.

The CVE with id CVE-2021-23173 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.847 and modified on date 2022-08-30T18:16:26.143. The vulnerability is described as The affected product is vulnerable to an improper access control, which may allow an authenticated user to gain unauthorized access to sensitive data.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-23543 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:16.963 and modified on date 2022-01-13T18:39:38.723. The vulnerability is described as All versions of package realms-shim are vulnerable to Sandbox Bypass via a Prototype Pollution attack vector.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-23568 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.043 and modified on date 2022-01-13T19:58:24.690. The vulnerability is described as The package extend2 before 1.0.1 are vulnerable to Prototype Pollution via the extend function due to unsafe recursive merge.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-23594 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.117 and modified on date 2022-01-13T19:06:05.193. The vulnerability is described as All versions of package realms-shim are vulnerable to Sandbox Bypass via a Prototype Pollution attack vector.. It has severity HIGH with exploitability score 10.0 and impact score 6.4.

The CVE with id CVE-2021-30360 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.190 and modified on date 2022-01-14T16:43:21.767. The vulnerability is described as Users have access to the directory where the installation repair occurs. Since the MS Installer allows regular users to run the repair, an attacker can initiate the installation repair and place a specially crafted EXE in the repair folder which runs with the Check Point Remote Access Client privileges.. It has severity HIGH with exploitability score 3.9 and impact score 10.0.

The CVE with id CVE-2021-32996 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.270 and modified on date 2022-01-13T20:44:50.017. The vulnerability is described as The FANUC R-30iA and R-30iB series controllers are vulnerable to integer coercion errors, which cause the device to crash. A restart is required.. It has severity HIGH with exploitability score 10.0 and impact score 6.9.

The CVE with id CVE-2021-32998 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.337 and modified on date 2022-03-21T17:58:31.550. The vulnerability is described as The FANUC R-30iA and R-30iB series controllers are vulnerable to an out-of-bounds write, which may allow an attacker to remotely execute arbitrary code. INIT START/restore from backup required.. It has severity HIGH with exploitability score 8.6 and impact score 9.2.

The CVE with id CVE-2021-34086 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.557 and modified on date 2022-01-14T15:08:21.370. The vulnerability is described as In Ultimaker S3 3D printer, Ultimaker S5 3D printer, Ultimaker 3 3D printer S-line through 6.3 and Ultimaker 3 through 5.2.16, the local webserver hosts APIs vulnerable to CSRF. They do not verify incoming requests.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-34087 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.613 and modified on date 2022-01-14T15:09:40.093. The vulnerability is described as In Ultimaker S3 3D printer, Ultimaker S5 3D printer, Ultimaker 3 3D printer S-line through 6.3 and Ultimaker 3 through 5.2.16, the local webserver can be used for clickjacking. This includes the settings page.. It has severity MEDIUM with exploitability score 8.6 and impact score 6.4.

The CVE with id CVE-2021-35247 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:17.667 and modified on date 2022-02-10T15:08:52.357. The vulnerability is described as Serv-U web login screen to LDAP authentication was allowing characters that were not sufficiently sanitized. SolarWinds has updated the input mechanism to perform additional validation and sanitization. Please Note: No downstream affect has been detected as the LDAP servers ignored improper characters. To insure proper input validation is completed in all environments. SolarWinds recommends scheduling an update to the latest version of Serv-U.. It has severity MEDIUM with exploitability score 10.0 and impact score 2.9.

The CVE with id CVE-2021-38894 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:20.410 and modified on date 2022-01-13T20:14:23.457. The vulnerability is described as IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 209515.. It has severity MEDIUM with exploitability score 8.0 and impact score 2.9.

The CVE with id CVE-2021-38895 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:20.470 and modified on date 2022-01-13T20:19:46.163. The vulnerability is described as IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209563.. It has severity LOW with exploitability score 6.8 and impact score 2.9.

The CVE with id CVE-2021-38921 and source identifier nvd@nist.gov was originally published on date 2022-01-10T14:10:20.527 and modified on date 2022-01-13T20:22:52.300. The vulnerability is described as IBM Security Verify 10.0.0, 10.0.1.0, and 10.0.2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM