Known Security Issues

The following is a list of known EdgeX security issues and vulnerabilities – and any associated Common Vulnerabilities and Exposures (CVE) reports to accompany the issue. CVE is a program for identifying, cataloging and addressing software and firmware vulnerabilities (see https://cve.mitre.org/). Nation ally, the federal government runs the CVE program to help build a free, standardized list or dictionary of security vulnerabilities for organizations to use to improve their software's exposure and posture to security threats.

EdgeX grades security issues on the CVSS(Common Vulnerability Scoring System) scale. The four levels are critical, high, medium and low level issues.

Component	Description	Severity	Affected Releases	Issue Link	Fix Timeline	Resolution/Mitigation
Database - MongoDB	MongoDB is one of the data persistence solutions useable in EdgeX. The MongoDB 3.4.9 container base image has known vulnerabilities stemming from its underlying base Linux image and some from MongoDB source itself..	Medium	Delhi Edinburgh	https://www.cvedetails.com/vulnerability-list/vendor_id-12752/product_id-25450/version_id-229891/Mongodb-Mongodb-3.4.9.html	Fuji	Pulling 4.0-xenial MongoDB package, which starts with a Debian base image that does not include a host of insecurities spanning Perl, OpenSSL etc, and some MongoDB specific fixes. https://github.com/edgexfoundry/docker-edgex-mongo/commit/2c86e5e4359367177dc339556604c3af6fb9ee2a
Database access credentials in the clear	MongoDB and Redis are the available data persistence layers in EdgeX. While the access credentials (username and password) are in the clear for MongoDB, located in the configuration service (aka Consul) or on the local file system, Redis defaults to no authentication.	High	Delhi Edinburgh		Fuji	EdgeX-using organizations should turn on the database access controls and institute a means to secure the data access credentials provided to the services. The issue has been resolved in EdgeX Fuji with credentials being created on the fly, saved in Vault and used during setup. Requires user to set secure mode on.
Go net package vulnerabilities	net/http: Denial of Service vulnerabilities (ping and reset) in the HTTP/2 implementation and net/url in Go before 1.11.13 and 1.12.x before 1.12.8 mishandles malformed hosts in URLs, leading to an authorization bypass in some applications. This is related to a Host field with a suffix appearing in neither Hostname() nor Port(), and is related to a non-numeric port number.	High, High, Critical	Delhi Edinburgh	https://nvd.nist.gov/vuln/detail/CVE-2019-9512 https://nvd.nist.gov/vuln/detail/CVE-2019-9514 https://nvd.nist.gov/vuln/detail/CVE-2019-14809 CVE-2019-9512 and CVE-2019-9514, and Go issue golang.org/issue/33606. net/url: parsing validation issue CVE-2019-14809 and Go issue golang.org/issue/29098.	Fuji	
Docker: edgexfoundry/device-coap{-arm64}:2.0.0	Multiple vulnerabilities due to accidental use of an obsolete base image	12 High, 4 Medium, each	Ireland	No issue filed	Ireland (patch)	Will republish edgexfoundry/device-coap{-arm64}:2.0.1 with updated base image or manually update Dockerfile use alpine: 3.12 or later and rebuild.
GitHub: edgexfoundry/*/go.mod	Vulnerabilities in golang.org/x/crypto/ssh	Numerous High	Ireland	CVE-2020-9283 (improper signature verification)	Indeterminate (no fix available)	SSH module is not directly used by EdgeX is not impacted by the vulnerability. Additionally, the vulnerable package is pulled in through multiple dependency chains using a pseduo-version number. Not fixable until patch is available in a direct dependency of EdgeX.
GitHub: edgexfoundry/*/go.mod	Vulnerabilities in golang.org/x/text	High	Ireland	CVE-2020-14040 (denial of service)	Indeterminate (no fix available)	EdgeX does not directly call the vulnerable functions (UseBOM, ExpectBOM). Additionally, the vulnerable package is pulled in through multiple dependency chains using a pseduo-version number. Not fixable until patch is available in a direct dependency of EdgeX.
GitHub: edgexfoundry/*/go.mod	Vulnerabilities in github.com/dgrijalva/jwt-go	High	Ireland	CVE-2020-26160 (access restriction bypass)	Indeterminate (no fix available)	Not exploitable. This library is used by EdgeX to generate JWT tokens for the API gateway. Token parsing (where the defect lies) is handled by the gateway (Kong). Thus, we are not susceptible.

GitHub: edgexfoundry/*/go.mod	Vulnerabilities in github.com/miekg/dns	High	Ireland	CVE-2019-19794 (insecure randomness)	Indeterminate (no fix available)	Dependency chain is at least 5 components deep. Unknown if exploitable. Not fixable until patch is available in a direct dependency of EdgeX.
Docker: edgexfoundry/*(-arm64):2.0.[01]	Vulnerability in Alpine 3.12 base image	Critical	Ireland	CVE-2021-36159 (out-of-bound read by libfetch)	Jakarta	Not expoitable. EdgeX foundry binaries are statically linked and do not have runtime dependencies on libfetch. Can be fixed locally by upgrading base image to latest Alpine version.
Docker: edgexfoundry/sys-mgmt-agent(-arm64):2.0.*	Vulnerability in docker:20.10.8 base image	High	Jakarta	SNYK-ALPINE314-OPENSSH-1728379	TBD	Not exploitable. ssh-keygen not used by sys-mgmt-agent.
GitHub: github.com/edgexfoundry/app-functions-sdk-go/v2	Broken encryption in app-functions-sdk “AES” transform in EdgeX Foundry releases prior to Jakarta allows attackers to decrypt messages via unspecified vectors	Low	<= Ireland	CVE-2021-41278	Jakarta	Broken crypto in in the app-functions-sdk "AES" transform results in a level of protection significantly less than the user would expect. As the broken transform is a library function that is not invoked by default, users who do not use the AES transform in their processing pipelines are unaffected. Those that are affected are urged to upgrade to the Jakarta EdgeX release and modify processing pipelines to use the new "aes256" transform.
Any EdgeX microservice that supports the /api/v2/config endpoint and supports connection to the EdgeX message bus (almost all of them).	Configuration API in EdgeXFoundry 2.1.0 and earlier exposes message bus credentials to local unauthenticated users	Moderate	<= Jakarta	CVE-2022-31066	Jakarta (2.1.1) Kamakura	The defect is resolved in Jakarta (2.1.1) and Kamakura (2.2.0) by injecting the message bus credential into a copy of the configuration structure that is not exported via the /api/v2/config endpoint.
Practically everything (introduced via go-mod-core-contracts)	Parse() can panic due to improper index calculation.	Medium	<= Jakarta	SNYK-GOLANG-GOLANGORGXTEXTINTERNALLANGUAGE-2400718 (CVE-2021-38561) (out of bounds read)	Levski	Not vulnerable. Requires test for "bcp47_language_tag" to trigger condition, which EdgeX does not check for. Otherwise, harmless to upgrade go-playground/validator.
Denial of service caused by panic() when parsing malformed Yaml	When uploading a device profile, malformed yaml can cause the core-metadata service to panic()	Medium	Jakarta 2.1.1	SNYK-GOLANG-GOPKGINYAMLV3-2841557 (CVE-2022-28948)	Fixed in Levski. Queued for Jakarta 2.1.2.	We calculated a modified CVSS score of between 3.3 and 6.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H), which is Medium severity, based on the following mitigating factors: (a) access to localhost or access via API gateway is needed and (b) presence of restart flags on core-metadata services.
DTO parsing (go-mod-core-contracts)	CPU usage vulnerabilty in parsing Accept-Language HTTP header	Medium	< Levski	SNYK-GOLANG-GOLANGORGXTEXTLANGUAGE-3043869 (CVE-2022-32149)	Awaiting upstream fix	Not vulnerable. Usage is here https://github.com/edgexfoundry/go-mod-core-contracts/blob/main/common/validator.go and we do not use the vulnerable parser.
API Gateway, containers	Vulnerability in certificate parsing can allow remote code execution.	High	< Levski	CVE-2022-3602 (OpenSSL advisory)	No fix required	Not vulnerable 2X. Reason 1: The vulnerability applies to openssl 3.x versions only, and our Alpine-based images use 1.x. Reason 2: Our alpine-based container images used 1.x versions. Even if it applied, the advisory states that for client to attack the server, the server must request TLS client authentication: EdgeX does not configure TLS client authentication. For clients connecting to servers, EdgeX services use golang crypto libraries not openssl. libssl is coincidentially included in our Apline-based container images, but this does not have an impact on EdgeX's services, which are written in golang.