# Security Notification
# SN 2021-07-26

26 July 2021

## Open memory dump method leaking customer information, secret keys, password , source code & admin accounts

**This article contains:**

- Summary
- Potential Vulnerability Synopsis
- Affected Products
- Resolution Description
- Appendix: About CVSS

**To mitigate the risk:**

- Follow Resolution Description procedure.

**It applies to:**

"Affected Products and Versions" section of this notice

---

## Summary

This security notification addresses an open memory dump vulnerability in the web url:

https://us.connectedplant.honeywell.com/actuator/env.

Actuator endpoints allow you to monitor and interact with your Spring application. Spring Boot includes a number of built-in endpoints and you can also add your own. Honeywell has remediated this vulnerability as described in the "Mitigating Factors" section to ensure this potential vulnerability is mitigated.

## Vulnerability Synopsis

This vulnerability allows any attacker to perform many severe attacks such as:

- Upgrade accounts without payments.
- Get logged in customer information and get access to the session & JWT tokes to take over accounts
- PII Data leaking
- Accessing all credentials from the application properties such as, admin credentials, swagger credentials, billing credentials.
- Get database credentials
- Server Environment variable
- Server config Properties.
- Payments manipulations and money stealing
- and more

**CVSS Base Score: 8.1 (High)**

**CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H**

## Affected Products and Versions

The potential vulnerability affects the following product versions: https://us.connectedplant.honeywell.com/actuator/env

All management endpoints are exposed by the developer mistakenly. Actuator is mainly used to expose operational information about the running application — health, metrics, info, dump, env, etc.

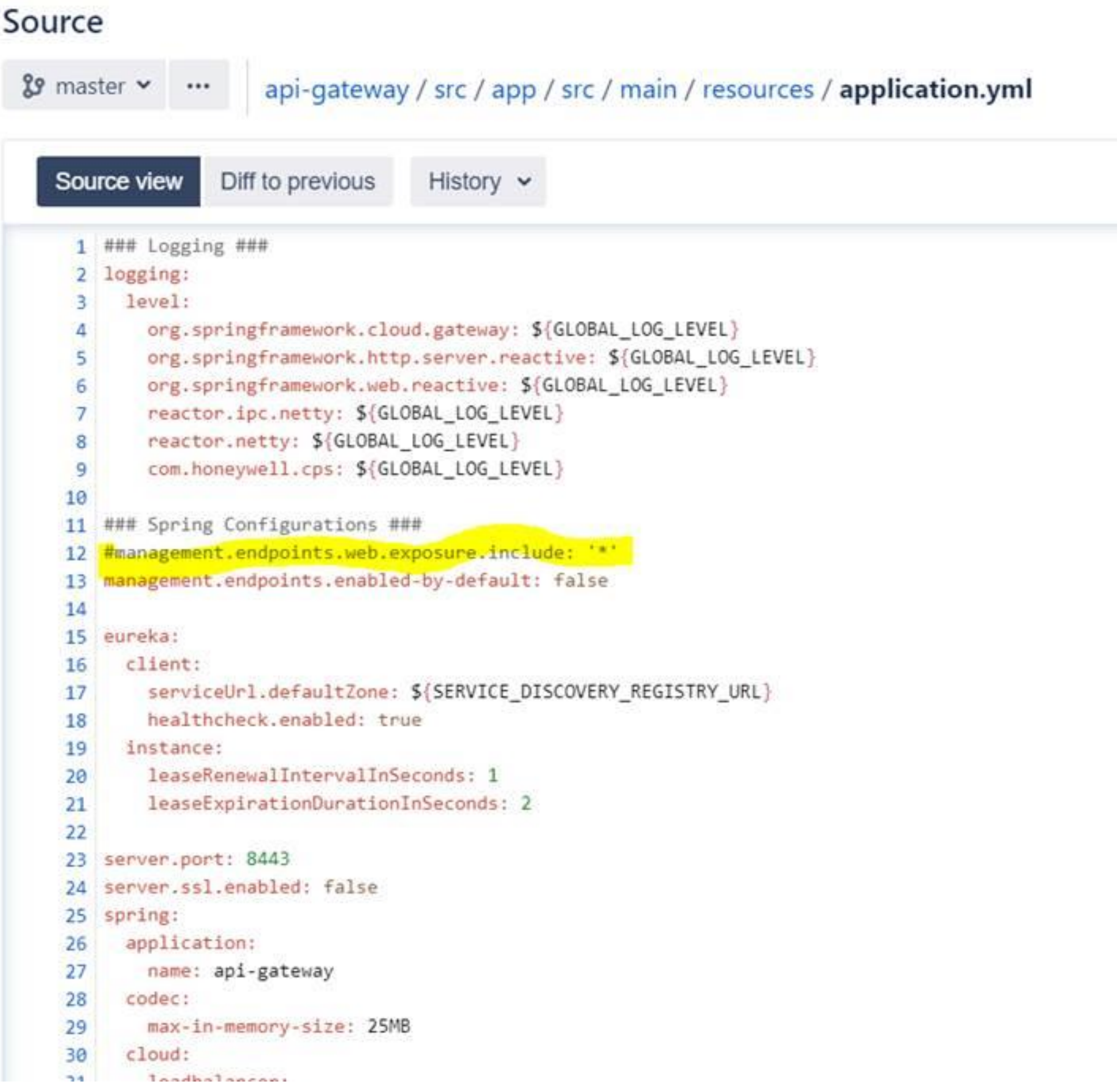
Information exposed:

- Environment Variables
- Internal service address
- AppID & Secret
- User Token: User token is valid for 60 mins. This is an issue if the heap dump is downloaded during active user session.

## Mitigating Factors

Honeywell has disabled endpoints and generated new secrets:

1. **Endpoints disabled**


Source
master
...
api-gateway / src / app / src / main / resources / application.yml
Source view
Diff to previous
History

```
### Logging ###
logging:
  level:
    org.springframework.cloud.gateway: ${GLOBAL_LOG_LEVEL}
    org.springframework.http.server.reactive: ${GLOBAL_LOG_LEVEL}
    org.springframework.web.reactive: ${GLOBAL_LOG_LEVEL}
    reactor.ipc.netty: ${GLOBAL_LOG_LEVEL}
    reactor.netty: ${GLOBAL_LOG_LEVEL}
    com.honeywell.cps: ${GLOBAL_LOG_LEVEL}

### Spring Configurations ###
#management.endpoints.web.exposure.include: '*'
management.endpoints.enabled-by-default: false

eureka:
  client:
    serviceUrl.defaultZone: ${SERVICE_DISCOVERY_REGISTRY_URL}
    healthcheck.enabled: true
  instance:
    leaseRenewalIntervalInSeconds: 1
    leaseExpirationDurationInSeconds: 2

server.port: 8443
server.ssl.enabled: false
spring:
  application:
    name: api-gateway
  codec:
    max-in-memory-size: 25MB
  cloud:
```

2. **Generating new secrets**

Secrets should always have a valid expiration and regenerated every six months.

## Resolution Description

Honeywell team has blocked the DNS to URL and app secret regenerated.

## Acknowledgments

This issue has been identified through PSIRT.

## Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The severity of the score can be summarized as follows:

| Severity Rating | CVSS Score |
|---|---|
| **None** | 0.0 |
| **Low** | 0.1 – 3.9 |
| **Medium** | 4.0 – 6.9 |
| **High** | 7.0 – 8.9 |
| **Critical** | 9.0 – 10.0 |

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Detailed information about CVSS can be found at http://www.first.org/cvss.

## DISCLAIMERS

3. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
4. YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
5. HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
6. HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
7. IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.