# Security Update:Cisco has released a security advisory to address HIGH vulnerabilities in Network Assurance Engine (NAE)

Cisco has released a security advisory to address HIGH vulnerabilities in Network Assurance Engine (NAE)

## Status Type

Security Update

## Private

Public

## Date and Time

Thursday, February 14, 2019 - 13:50

## Reason

Security update

## Impact

Cisco users

### WHAT HAPPENED

Cisco has released a security advisory to address **HIGH** vulnerabilities in Network Assurance Engine (NAE).

**Advanced Users:** For a complete description of the vulnerabilities and effected systems, visit:

- **Cisco Network Assurance Engine CLI Access with Default Password Vulnerability** at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190212-nae-dos [1]

**AFFECTED SYSTEM - Versions:**

- **Cisco Network Assurance Engine (NAE) Release 3.0(1)**

**WHAT?S THE PROBLEM?**

An attacker could exploit this vulnerability to obtain sensitive information.

**WHAT DO I NEED TO DO?**

Users and administrators are encouraged to go to the link listed above and review the Cisco Security Advisory.

**RELATED LINKS**

https://it.ucsf.edu/security [2]



---

**Source URL:** https://it.ucsf.edu/status/2019-02-14/cisco-has-released-security-advisory-address-high-vulnerabilities-network

**Links**
[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190212-nae-dos
[2] https://it.ucsf.edu/security