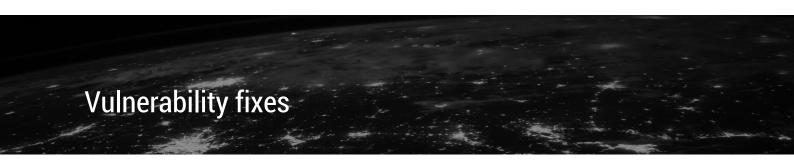


Maximize uptime. Develop insights. Provide answers.



Date: 17 Dec 2019

Vulnerability Status: Fixed

Severity/Risk: Medium

Category: Web Servers

Type: Attack

Summary: The hard session limits the amount of an attacker can use a hijacked session and impersonate the victim user. This weakness can arise on design and implementation levels and can be used by attackers to gain unauthorized access to the application.

## Solution:

• Set the hard timeout to 4 hrs.

NetGain EM Affected Version/s: NetGain EM FMI, DEMO, STANDARD/PLUS with versions:

- v7 7.2.1067b179 and below
- v10 10.1.162\_b954 and below

## References:

- https://www.immuniweb.com/vulnerability/insufficient-session-expiration.html
- <a href="https://cwe.mitre.org/data/definitions/613.html">https://cwe.mitre.org/data/definitions/613.html</a>