March 28, 2019 | Issue # 20

# Information Security

**TOPIC: Vulnerability Management and Patching**

***This is the last newsletter in the DefSec series. Thank you for subscribing!***

Vulnerability Management (VM) is a security practice designed to proactively prevent the exploitation of Information Technology (IT) vulnerabilities that can exist within an organization. An organization's security policy should mandate that VM activities take place within the organization.

Vulnerabilities should be rated and prioritized, so as to take appropriate remediation actions. There are number of sources a VM team can use to discover vulnerabilities, some sources include; Canadian Centre for Cyber Security (CCCS), CERTs, Vendors or Security News Feeds (RSS). Upon receiving a vulnerability notification, the VM team should analyze and validate the vulnerability to determine relevance and criticality. According to the DefSec control objective in this area, high and critical vulnerabilities must be remediated through patching, decommission or compensating controls should be applied to reduce the risk of exploitation.

VM activities must include Patching. It is important for IT systems to have the functionality to rollback patches, in case an installed patch negatively impacts another (critical) system. Patching should be timely and relevant, meaning the right patch version should be applied at the right time based on criticality.

**UPCOMING SECURITY EVENTS:**

- **BC Security Day: June 13, 2019**
  *The Province organizes two "Security Day" events annually, admission is free of charge and you can either attend in-person or via webcast. At the event, experts in the field of security present and discuss topics pertaining to advancement in technology and security implications. Join us for the 2019 spring Security Day and learn about "Smart Cities"; check our website for more information: http://www.gov.bc.ca/securityday.*