CRC
CENTER for RESEARCH COMPUTING

CRC System Security

Vulnerability and Compromise Resolution Policy

It is the responsibility of the system administrators (**primary and backup**) to keep their computational service (physical, VM or container) up-to-date with the latest system and application security patches. All services are scanned on a weekly basis by the Qualys and OpenVAS tools, in coordination with the ND OIT Information Security team. In the event that a compromise, critical or high security vulnerability, or End-of-Life (EOL) operating system is identified, the policy outlined below is followed.

- Step 1
    - CRC operations staff will contact the designated system administrators via e-mail, explain the security finding and ask them to resolve the security vulnerability.
- Step 2
    - A: When an administrator responds to the e-mail, CRC staff will explain the network restriction policies and work with the administrators toward resolution
    - B: If no response is received from the designated administrators according to the timetable below, then the designated action will be taken.

Compromised Service (VM will be used as reference example):

If a VM is determined to be compromised via scan or external “abuse” reports it will be immediately removed from the campus network (access only via select IP addresses).

Level 5 (critical) severity vulnerabilities:

- VM will be removed from the public DNS by end of current business day
- After 48 hours, VM is turned off. VM will be started back up when a plan is arranged between CRC staff and VM administrators to resolve the security vulnerability

Level 4 (high) severity vulnerabilities and EOL operating system:

- After 48 hours, VM will be removed from the public DNS
- After one week, VM is turned off. VM will be turned back on when a plan is arranged between CRC staff and VM administrators to resolve the security vulnerability

Note 1: The levels described above correspond to the levels provided by Qualys. There may be situations where the severity of a vulnerability is treated by CRC or OIT as higher or lower.

Note 2: In the case where a vulnerability shows up in an EOL version of software (where patches are not available), CRC directors will determine how to fund software upgrade.

Note 3: This policy applies to services on the CRC network range. Services in a DMZ, Cloud, ND OIT or other non-CRC platform are governed separately.

Note 4: CRC operations staff will provide initial VM OS configured to CRC security best practices.