Patch Management Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Reviewed Date – 06/07/2024

1. Purpose

Ensure information systems attached to the District of Columbia Government (District) network is updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits.

2. Authority

DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer (OCTO) with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District government. This document can be found at https://code.dccouncil.gov/us/dc/council/code/sections/1-1402.

3. Applicability

This policy applies to all the District's workforce members performing official functions on behalf of the District's government, and/or any District agency/entity that receives enterprise services from the OCTO. In addition, this policy applies to any provider and third-party entity with access to the District's information, systems, network and applications.

4. Policy

District agencies must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. OCTO will review, update, and disseminate this policy annually at a minimum, to ensure accuracy, clarity, and completeness. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. Frequently checking the network health status:

4.1.1. Identify missing patches, computer vulnerabilities due to missing patches, failed patches, etc.
4.1.2. Maintain an inventory of production systems, types of operating systems, roaming computers, remote office machines under IP scope management, etc.
4.1.3. Manage 'bring your own device' (BYOD) components, including laptops used for work that are not District-owned or managed.
4.1.4. When new computers are added to the network, make sure that the new system is covered under automated patching.
4.1.5. Be aware of certain patches that shouldn't be deployed in the network as they may prevent other components from operating efficiently, some versions of Java RE, for example.

4.2. Evaluating Patches in a test environment before applying to the Production environment:

The test environment should mirror the network, containing the same types of operating systems and applications used in production. Testing patches before deployment ensures that it is stable for deployment. This process is replicable for the whole enterprise.

4.3. Developing a Patch Management Program that ensures that Systems, Utilities, and Applications are regularly patched:

4.3.1. A regular schedule (30 days for Levels 5 & 4 and 90 days for level 3) must be developed for security patching of all the District systems and devices.

4.3.2. Patching must include updates to all operating systems, including office productivity software, database software, and third-party applications (e.g., Firefox, Java RE, etc.), under the direction of OCTO management.

4.3.3. Where vendors have automated patching procedures for their applications, automatic updates must be enabled on the systems for such applications.

4.3.4. OCTO makes use of appropriate patch management software or tools to support the patching process across many different platforms and devices. Agencies whose devices are not supported by OCTO are encouraged to adopt the tool approved by OCTO.

4.3.5. OCTO performs regular reviews of the application of critical security patches as part of the agency's change management and audit functions.

4.4. Device types:

4.4.1. Workstations (Stationary and Mobile): Desktops and laptops must have automatic updates enabled for operating system patches. Any exception to the policy must be documented and forwarded to OCTO for review.

4.4.2. Servers: Servers must be regularly updated with the latest service packs, hotfixes, and patches required to ensure the security of the asset and the data that resides on the system, except for cases where the deployment of such patches will obstruct the normal operation of Applications hosted on the server. Any exception to the policy must be documented and forwarded to the Office of the CISO and OCTO for review.

4.4.3. Third-Party Supplied and Managed Devices: All IT devices being supplied and managed by Third Parties must have up-to-date security patches before going operational. Third Parties must provide evidence of up-to-date patching before the devices are accepted into service and become operational.

4.5. Generate detailed patch summary reports:

IT reports are important for security auditing. Patch deployment summary reports can be generated, which are essential in risk assessment and helps ensure vulnerabilities are addressed.

4.6. Patching exceptions:

Patches on production systems (e.g., servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through a risk assessment process. Reasons for any departure from the above standard and alternative protection measures taken must be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require the approval of the District CISO.

5. Exemption

Exceptions to this policy shall be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO) for approval.

6. Definitions

The definition of the terms used in this document can be found in the *Policy Definitions website*.