INFORMATICA SECURITY VULNERABILITY PATCHING POLICY V1

Overview

Informatica's goal is to ensure that our customers are provided with high level protection against identified vulnerabilities and to produce appropriate fixes in a timely manner. Depending on the unique attributes of a given security vulnerability, Informatica's fix may be in the form of a software update, either as a patch or a scheduled version release. In addition, Informatica works to ensure that disclosure methods of vulnerabilities are performed through appropriate channels to our customer community.

Computer systems owned or licensed by Informatica or its suppliers for the Cloud Service or Support Service ("Informatica Systems") implement and maintain software designed to detect and prevent malicious code that may perform unauthorized functions or permit unauthorized access to any Informatica System, including computer viruses, Trojan horses, worms, and time bombs.

Vulnerability Priorities and Assessment

Upon discovery of a security vulnerability, a process of assessment and analysis commences and may vary depending on the vulnerability attributes. Security vulnerability assessments are performed by our Product Security and Product Management teams and include the evaluation of the risk and potential mitigation. Informatica determines remediation priority based on Common Vulnerability Scoring System (CVSS) v3 severity score and other contextual factors including exposure, applicability, and impact of the potential threat or vulnerability. The assessed priority of a vulnerability may be reduced or raised from its raw CVSS severity score due to these contextual factors.

Priorities:

Critical – A vulnerability that could be easily exploited by a remote unauthenticated attacker and may lead to system compromise without requiring user interaction resulting in the loss of confidentiality, integrity, or availability of the system or data.

High - A Vulnerability that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.

Medium - A vulnerability that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources, under certain circumstances. These are the types of vulnerabilities that could have an impact but are less easily exploited based on a technical evaluation of the flaw or affect unlikely configurations.

Low - All other issues that have a security impact. These are the types of vulnerabilities that are believed to be unlikely to be exploited, or where a successful exploit would have minimal consequences.

Security Vulnerability Treatment Response

Informatica's response to identified security vulnerabilities is determined by the risk and severity ratings calculated during the vulnerability assessment. Mitigation times detailed below represent target goals.

For all Cloud Services, except Type II Cloud Services identified as "Cloud Edition", Informatica starts mitigation of critical priority vulnerabilities in Informatica proprietary components within forty-eight (48) hours of determining priority and uses commercially reasonable efforts to remediate within the next monthly release window. Informatica starts mitigation of high priority vulnerabilities within seven (7) days of determining priority and uses commercially reasonable efforts to remediate within the next monthly release window. Informatica uses commercially reasonable efforts to remediate medium priority vulnerabilities within the next three (3) monthly release windows and to remediate low priority vulnerabilities within the next six (6) monthly release windows. The "release window" is the time period during which a release is implemented across Informatica Systems and the "next monthly release" is the release immediately after that in which the vulnerability was first confirmed to be present. Mitigations and remediations are deployed by Informatica, except that mitigations and remediations for the Informatica Cloud Secure Agent may be delivered initially as EBFs, which the customer is responsible for deploying based on their maintenance window availability.

For Type II Cloud Services identified as “Cloud Edition”, Informatica starts mitigation of critical priority vulnerabilities in Informatica proprietary components within forty-eight (48) hours of determining priority and uses commercially reasonable efforts to remediate within thirty (30) days. Informatica starts mitigation of high priority vulnerabilities within seven (7) days of determining priority and uses commercially reasonable efforts to remediate within thirty (30) days. Informatica uses commercially reasonable efforts to remediate medium priority vulnerabilities within six (6) months of determining priority and to remediate low priority vulnerabilities on a commercially reasonable basis. Mitigation and remediation may be via updates, upgrades, patches, or bug fixes for Cloud Edition software, which Informatica will make available for implementation by or on behalf of Customer. Customer is responsible for its decision to delay implementation.

For vulnerabilities in third party and open-source components, Informatica follows the same remediation schedules upon release of the applicable patch by the third party or open-source vendor.