及时更新 Toad® by Quest®，确保数据安全无虞

关于 Toad for Oracle 内置软件安全标准的技术简介

作者：Quest Software 高级产品经理 Julie Hyman 和产品营销经理 Ryan Crochet, Sr.

在当今网络安全威胁愈演愈烈的环境下，无论当前采用何种安全协议或体系结构，IT 管理员都必须对桌面和网络上允许存在哪些软件划定明确的界限。采用独特组合的新型勒索软件攻击和恶意活动不断增加，加之组织依赖使用各种软件和应用程序来实现业务成果，使得组织必须积极主动、坚持不懈地进行软件管理。若要保护组织的数字资产，首要任务是满足下面两项最低要求：

1. 仅安装安全的软件
2. 持续更新软件，以确保系统的安全

在本技术简介中，您可以找到对这两项要求的支持，从而为您供应链软件的安全性提供保障。

软件供应链安全性

软件供应链的安全性是指软件组件及其依赖关系在整个软件开发生命周期（从创建到部署）内的完整性、机密性和可用性。这一点至关重要，因为一旦软件组件遭到入侵，就可能会危害整个组织及其客户。有效的软件供应链安全措施通过在整个流程中提供可见性、控制和保障，有助于更大程度地降低此类风险。

继续阅读，了解有关以下方面的更多详细信息：

- **什么是软件供应链安全性，它对您有何重要意义**
- **及时更新软件的重要性**
- **有助 Toad 保护您安全的重要安全控制措施**

数据安全与 TOAD

Toad by Quest 是一个集成式开发环境 (IDE)，支持开发人员和数据库管理员创建、管理和维护数据库，包括角色和用户。一旦攻击者获得了对用户 Toad 会话的访问权限，便可能执行未经授权的数据库命令，窃取敏感数据，甚至使整个数据库陷于瘫痪。因此，务必确保定期更新、正确配置并采取适当的安全控制措施来保护 Toad 及其关联的组件，以降低这些风险。备注：无论当前采用何种体系结构和安全协议，操作系统和数据库平台本身都是需要保持最新状态的关键组件。同样地，这也包括 Database IDE 的组件，因为 IDE 及其关联组件中的任何安全漏洞，都可能危及整个数据库环境的安全。

应用程序安全与更新 TOAD

接下来，考虑一下您在持续更新软件以确保网络安全方面所承担的角色。利用 WannaCry/Petya 漏洞发起的勒索软件攻击表明，全球有数十万台计算机在运行过时的软件。（当中很多计算机至今仍是如此。）虽然 WannaCry 修复程序已作为 Windows 正常更新的一部分予以分发，但很多公司并未应用此更新。尽管警告持续了数月之久，但 Petya 利用同一漏洞发起了第二波攻击，尚未更新的计算机深受其害。

诚然，有些 IT 团队会延迟更新，因为更新会迫使系统重新启动并影响生产力；有些人担心更新会影响数千计用户所依赖的应用程序；有些人只优先执行一些必要的更新，且何为“必要”由他们自行定义；还有些人对更新 Toad 及其他开发软件抱持“未损勿修“的态度。

已识别的漏洞

以下示例说明用户为何需要留意并使用最新支持的版本。几年前，在构建 / 发布版本期间的定期检查过程中，Quest 识别并解决了 Toad for Oracle v13.1.1 中的一个漏洞，并发出了以下通知：

“Quest 最近修补了其中一个 [第三方] 库，我们在此库中发现了一个关键漏洞 (CVSS 9.3)。该漏洞影响到 Microsoft Visual C++ 库，并可能导致权限升级。我们最新版本的 Toad 已修复此漏洞。”

若您读到这里并认为，“它可以和我需要的 Oracle 版本协同工作，这有什么问题？”

它可以和我需要的 Oracle 版本协同工作，这有什么问题？”

首先，10 年前发布的软件能够与 9 年后发布的数据库协同工作，不是很好吗？如今，向前兼容并不常见。

其次，从网络安全的角度来看，无论采用哪种体系结构，或者使用何种安全协议或防火墙，这都不是最佳实践。如果仍在使用已不再享受支持服务的软件，则由于无法应用任何更新或修补程序，它们会更容易遭受安全威胁，进而可能损害与之交互的数据的完整性和机密性。随着专有软件越来越多地采用开源库，网络威胁的来源亦日益增加。

2018 年，Fossa 进行的一项研究发现，92 % 的软件项目都是使用开源组件，平均每个应用程序包含 57 % 的开源代码。2019 年，Synopsys 同样发现，在其分析的专有应用程序的代码中，开源代码平均占 70 %。

接下来，我们以 2021 年 Log4j 危机为例予以说明。Log4j 网络威胁是由 Apache Log4j 库中的一个漏洞所造成，Apache Log4j 库是一种广泛使用的 Java 应用程序开源日志记录工具。此漏洞使得攻击者能够在受感染的系统上远程执行恶意代码，从而可能导致数据失窃、勒索软件攻击及其他安全漏洞。

log4j 漏洞影响了世界各地的大量组织，其利用的速度和范围引起了人们对开源软件安全性的担忧，并亟需采取更强有力的网络安全措施。

简而言之，若无软件物料清单，您永远无法真正了解软件存在的依赖关系，也永远无法真正知道下一个威胁来自何处。您唯一的保障措施就是使用受支持的软件，并在下一个威胁出现时安装可用的修补程序。

因此，再问一次，您知道自己使用的 Toad 版本及其是否受支持吗？一直以来，Quest 不断发布更新、更安全的版本。下面我们举个例子。表 1 列出了 Toad for Oracle 的部分版本记录。对于所有低于 15.0 的版本，均已停止提供支持服务。

新版 Toad 产品，例如 Toad for Oracle，不仅对功能进行了改进，还大幅提高了安全性。通过我们的发布流程，Toad 紧跟数据库开发过程中千变万化的漏洞与威胁局势，不断地演进与发展，其中包括：

- 与数据库的连接不安全（未加密）
- 意外权限升级（例如低权限用户升级至超级用户）
- 针对访问存储在云端的个人身份信息 (PII) 和敏感数据所设立的门槛过低
- PII 被存储（并被遗忘）在数据库的非生产副本中

Quest 的客户一年至少有两次机会将 Toad 更新至最新版本，并增添安全改进措施来缓解此类威胁。

Toad for Oracle 版本与支持

版本	支持	正式发布日期
16.3	全面支持	2023 年 4 月 7 日
16.2	全面支持	2022 年 9 月 30 日
16.1	有限支持	2022 年 6 月 29 日
16.0	有限支持	2022 年 4 月 26 日
15.1	有限支持	2022 年 1 月 27 日
15.0	有限支持	2021 年 10 月 18 日
14.2	已停止支持	2021 年 7 月 13 日
14.1	已停止支持	2021 年 3 月 30 日
14.0	已停止支持	2020 年 10 月 23 日

表 1. 未列出的早期产品版本视为已停用。有关最新信息，请参阅 Toad for Oracle 的版本支持表。（此处）

为防范供应链攻击而采取的安全控制措施

在当今复杂的软件环境中，IT 管理员必须应对一系列安全挑战，包括需要解决跨多个应用程序和平台的各种漏洞。随着开源库在软件开发中的使用越来越广泛，识别并管理软件供应链中的依赖关系变得日益迫切。

有效管理软件依赖关系对于确保系统安全性，以及降低网络攻击风险或与许可问题相关的法律复杂性至关重要。为实现此目的，组织必须优先考虑供应链安全性，并实施相关策略，以便在整个软件开发生命周期中管理和监控依赖关系。

Quest 发现人们越来越担心供应链攻击，因为这意味着在面向客户发布产品之前，便已在其中引入恶意软件。为此，我们实施一系列扫描控制措施，以遵守软件安全标准，在 Quest 的 Toad 产品（包括 Toad for Oracle）构建流程中，识别并消除恶意软件。这些控制措施可确保产品没有漏洞和恶意软件，不包含隐藏的后门，并由秉持诚信行事的员工和承包商开发。表 2 显示每个版本 Toad 所采取的安全控制措施。

Toad 紧跟数据库开发过程中千变万化的漏洞与威胁局势，不断地演进与发展。

安全控制措施	描述
1. 安全培训	开发人员、经理和主管必须接受2.5小时的指定安全培训。
2. 安全软件开发生命周期	开发生命周期是根据Quest的信息与系统管理(ISM)业务部门的最佳实践而确定。
3. 第三方软件	在发布应用程序之前，会按照标准流程检查捆绑的第三方软件是否存在漏洞。
4. 漏洞扫描	使用符合行业标准的SAST/DAST产品对所有软件进行漏洞扫描。
5. 渗透测试（第三方）	每年都会对产品进行第三方渗透测试。
6. 恶意软件扫描	在发布所有产品之前，都会使用两个独立且符合行业标准的防恶意软件扫描程序进行恶意软件扫描。
7. 代码签名	分发给客户的软件都使用Quest的官方签名密钥进行加密签名，以验证真实性。
8. 软件完整性	发布软件安装程序的检验和，以便客户能确保所分发软件的完整性。
9. FIPS合规性	使用经FIPS批准的加密算法保护静态及传输中的敏感数据。

表 2：为抵御供应链攻击而在 Toad 中采取的安全控制措施

- 软件安全威胁
- 安全软件设计
- 安全编码
- 安全测试
- 安全与风险概述
- Web 客户端服务器交互代码问题
- 胖应用程序和客户端 - 服务器交互问题
- 加密和安全滥用问题
- 软件开发生命周期内的安全性

下文详细说明了 Quest Software 如何为 Toad 产品实施各项控制措施：

1. 安全培训

培训目标是制定安全知识基准，改进安全编码实践，以及提高对“Quest 安全软件开发生命周期”相关要求（参见下文）的遵守程度。目前涵盖的培训主题包括：

- 了解安全软件
- 软件安全威胁
- 安全软件设计
- 安全编码
- 安全测试
- 安全与风险概述
- Web 客户端服务器交互代码问题
- 胖应用程序和客户端 - 服务器交互问题
- 加密和安全滥用问题
- 软件开发生命周期内的安全性

Quest 会跟踪每门课程的完成情况并保留记录，以便在客户审核期间使用。记录表明 Quest 工程师团队接受过安全开发实践相关培训。

2. 安全软件开发生命周期 (SSDLC)

Toad 产品的 SSDLC 为产品本身的开发流程引入了安全与隐私注意事项。SSDLC 旨在帮助 Toad 工程师编写安全的软件、遵守软件安全标准并降低工程成本。SSDLC 的组件和阶段包括：

- 界定安全要求
- 定义指标和合规报告
- 执行威胁建模
- 定义并使用加密标准
- 管理使用第三方组件的风险
- 建立标准事件响应流程

3. 第三方软件和组件修补

像很多企业软件供应商一样，Quest 也经常纳入其他公司（下称“第三方”）编写的代码，这样 Quest 就无需从头开始重新创建代码。但随着时间的推移，一些第三方组件会出现漏洞，需要加以修补。除了依靠 NIST CVE 数据库获取当前漏洞的相关信息，Quest 还使用一些工具来识别第三方 DLL 以及可能在这些 DLL 中已发现的所有漏洞。Quest 还制定了一个流程，以降低发布带有易受攻击的第三方组件的软件的可能性。流程如下：

- 指定无载体漏洞的标准
- 要求提供产品所捆绑的第三方组件、软件和 DLL 的清单
- 要求定期检查第三方组件有无漏洞
- 规定第三方修补易受攻击的组件的最后期限（30 天 /60 天 /180 天）
- 要求在对产品进行了修补并发布了新版本时通知客户

4. 漏洞扫描（SAST 和 DAST）

Quest 针对使用外部工具进行 SAST（静态应用程序安全测试）和 DAST（动态应用程序安全测试）扫描，制定了相应的流程。

SAST 是一种白盒测试。使用 SAST 的测试人员会从内部检查应用程序，在其源代码中搜索有无指示可能存在安全漏洞的状况。DAST 是一种从外部进行的黑盒测试，就如攻击者看到应用程序一样。使用 DAST 的测试人员会在 Web 应用程序运行时对其进行检查，并尝试模拟攻击者对其进行攻击。

SAST 工具用于协助识别名为“常见缺陷枚举”(CWE) 的列表中所列的缺陷。此类工具在处理逻辑流、身份验证和授权等问题方面受到限制，更适合渗透测试（参见下文）或手动源代码审查。DAST 扫描程序从外部与 Web 应用程序交互，其依赖于 HTTP 且独立于技术。

对于 Toad 产品，此流程包括以下措施：

- 可能的情况下，使用目前指定的 SAST/DAST 工具，每年至少对产品 /Web 应用程序自动进行两次完整扫描，且在所有版本发布之前亦进行完整扫描
- 使用 SAST/DAST 工具对 Quest 开发的所有产品代码进行扫描
- Toad 安全顾问对每次扫描的结果进行审查，必要时与 InfoSec 总工程师合作，确定所发生问题的严重性
- 任何产品在发布时均没有严重或高级别漏洞
- 对于中低级别漏洞，安全顾问会与产品架构师合作处理
- 安全顾问和产品架构师针对扫描所发现的任何漏洞共同确定合适的解决方案

SAST 会从内部检查应用程序，在其源代码中搜索有无潜在安全漏洞。DAST 是一种从外部进行的黑盒测试，就如攻击者看到 Web 应用程序一样

5. 渗透测试（第三方）

渗透测试演示了漏洞或流程缺陷被攻击者利用时对现实世界产生的影响。其目的是在不良分子发起攻击之前评估安全性。渗透测试并不是对应用程序或其源代码进行自动扫描，而是自动漏洞扫描（参见上文）之后的下一步。

对于 Toad 产品，每年都会进行渗透测试。此类测试包含手动和自动测试，旨在维护产品在以下方面的软件安全标准：

- 应用逻辑
- 代码注入
- 本地存储
- 二进制利用与反向工程
- 权限过多
- 敏感信息存储未加密
- 敏感信息传输未加密
- 实施的加密技术安全系数低
- 汇编的控制措施安全系数低
- GUI 控制措施安全系数低
- 密码安全系数低或采用默认密码

大多数情况下，渗透测试遵循一个特定框架，具体取决于目标应用程序或基础架构；并且测试策略也因模拟的攻击者而异。

更新 Toad 的理由

通过渗透测试，Quest 识别并解决了 Toad for Oracle v13.3 中的一个漏洞，随后向客户发出如下通知：“在最近的渗透测试中，我们发现了一个问题，即当用户以不安全方式连接数据库时，系统未向用户发送通知。如果用户在不知情的情况下通过未加密链路连接到系统，攻击者则可捕获用户的凭据，或通过此连接传输的所有数据。Quest 已修复此缺陷。”

6. 针对软件版本的恶意软件扫描

当 Toad 产品版本打包发布时，首先会按照统一流程扫描它们是否存在恶意软件；该流程包含下列步骤：

- 扫描之前，使用 SHA-256 算法对安装包进行哈希计算，并且计算得出的哈希值必须与产品包上最终发布的哈希值相符。

在发布以供安装之前，所有软件版本都会经过扫描以查看是否包含恶意软件。

- 首先扫描安装程序中捆绑的所有文件是否含有恶意软件。
- 恶意软件扫描是自动执行的（使用命令行进程或脚本）。
- 使用独立的恶意软件扫描程序（两个用于 Windows，两个用于 Linux），并在扫描前使用最新的签名 / 定义进行更新。
- 每次扫描均生成证据记录，包括时间、日期和结果；该记录会永久保存。
- 产品包中的任何文件如有例外情况，须经由安全与工程主管审批。

此流程涉及多个软件安全标准，包括：

扫描之前，使用 SHA-256 算法对安装包进行哈希计算，并且计算得出的哈希值必须与产品包上最终发布的哈希值匹配

- 在发布以供安装之前，所有软件版本都会经过扫描以查看是否包含恶意软件
- 首先扫描安装程序中捆绑的所有文件是否含有恶意软件
- 恶意软件扫描是自动执行的（使用命令行进程或脚本）
- 使用独立的恶意软件扫描程序（两个用于 Windows，两个用于 Linux），并在扫描前使用最新的签名 / 定义进行更新
- 每次扫描均生成证据记录，包括时间、日期和结果；该记录会永久保存
- 产品包中的任何文件如有例外情况，须经由安全与工程主管审批

7. 和 8. 代码签名和软件完整性

应用程序带有 Quest 代码签名证书，便是向客户保证此应用程序确由 Quest 创建且软件可信。代码签名流程的目的是通过验证软件的作者来确保其真实性。它还通过证明代码自签名以来未曾被更改，来确保软件的完整性。代码签名在发布更新和修补程序方面也发挥着重要作用。当 Quest 使用原始应用程序中所用的相同密钥签署 Toad 产品更新时，即代表该更新可信；它不可能来自 Quest 以外的任何来源。最后，代码签名中生成的校验和可确保用户收到正确的文件，而非使用被盗密钥签名的文件。所有主要操作系统和 Web 浏览器都支持代码签名，以防分发恶意代码。

Quest 对安装程序中包含的每个 .exe 和 .dll 文件，以及与应用程序和安装程序文件本身一起打包的二进制文件进行签名。

9. 通过保障 FIPS 合规性来保护敏感数据

由于您的应用程序和数据库中存在敏感数据，因此会增加保护负担。敏感数据几乎涵盖您想防止落入不良分子之手的任何类型数据，包括：

- 网络凭据
- 密码
- 社会保障号
- 信用卡信息
- 个人身份信息 (PII)，例如姓名、地址和电话号码
- 个人健康信息 (PHI)
- 财务信息
- 内部记录
- 知识产权

Toad 产品系列通过符合美国政府邦联信息处理标准 (FIPS) 的加密算法来保护敏感数据。此外，他们对传输中的敏感数据和静态敏感数据都应用此保护措施。

FIPS 标准对基于加密技术的安全系统，包括加密方法和加密密钥生成方式，详细阐述了最佳实践和要求。FIPS 合规性是所有用于美国政府工作的计算机都须满足的一项强制要求，并且已拓展至测试将在美国政府所用计算机上运行的外部应用程序（如 Toad）。

所有 Quest 产品都符合经过 FIPS 批准的加密和哈希算法。每个版本发布之前，都会验证 FIPS 合规性的当前状态（目前为 FIPS 140-2）。

Toad 产品是使用以下一个或多个加密服务提供程序和库 / 类构建的：

- SHA-256 (.NET)
- DSA (.NET)
- RSA (.NET)
- ECDSA (.NET)
- AES (.NET)
- Java 加密类

所有 Quest 产品都符合经过 FIPS 批准的加密和哈希算法。每个版本发布之前，都会验证 FIPS 合规性的当前状态（目前为 FIPS 140-2）。

更新 Toad 的理由

通过 FIPS 140-2 合规性测试，Quest 识别并解决了 Toad for Oracle v13.2 中的一个漏洞，随后向客户发出如下通知：

“Quest 发现了一个活跃的漏洞，攻击者可利用此漏洞解密 Toad 产品中储存的凭据。该漏洞攻击利用 Toad 加密密码的方式，可用于解密并使用凭据，从而入侵受影响的数据库、FTP 服务器或 SSH 服务器。此后，Quest 实施了强加密策略，修补了此漏洞，并发布了该软件的不易受攻击版本。

解决软件安全标准

	安全培训	第三方软件和组件修补	漏洞扫描	针对软件版本的恶意软件扫描	代码签名和软件完整性
NIST SP 800-53 R4	✓	✓	✓	✓	✓
ISO 27001	✓	✓	✓	✓	
PCI DSS v3.0	✓	✓	✓		
PCI 1.4				✓	
AICPA TSC 2014		✓	✓		
AICPA TSC (SOC-2)				✓	
HIPAA 45 C.F.R.		✓	✓	✓	

总结

上文所述的安全控制措施旨在降低 Toad 产品的供应链安全风险。图 2 演示了其流程。

Toad 产品受到重视和信赖，已为数据库专业人员带来数百万小时的生产力提升。通过更新 Toad 产品，您可以确保持续获得新功能并遵守软件安全标准。您还会获得全面的技术支持，并确保组织的安全状态百密而无一疏。

图 2：Toad 产品开发的安全控制流程

作者简介

Julie Hyman 是 Quest Software 负责数据库工具产品组合的高级产品经理。她是一位经验丰富的软件产品经理，拥有 25 年在初创公司和《财富》500 强公司创建和改进软件产品的经验。多年来，Julie 一直与各行各业及众多优秀企业的数据库管理员、开发人员和分析师密切合作，以确保 Quest 继续提供卓越的解决方案。

Ryan Crochet 是 Quest Software 信息与系统管理部门的高级产品营销经理。秉持对其所服务市场及其经常面临的问题的热情，Ryan 不断想方设法来解决这些问题，同时展示并宣传数据驱动型决策的力量，如何通过协调技术专长来推动取得业务成果。

关于 Quest

Quest 致力打造软件解决方案，在日益复杂的 IT 环境中带来新技术的优势。从数据库和系统管理到 Active Directory 和 Microsoft 365 迁移和管理，乃至网络抗风险能力，Quest 倾力帮助客户立足当下，解决其面临的下一个 IT 挑战。在全球范围内，有超过 130,000 家公司和 95 % 的《财富》500 强企业依赖 Quest，凭借其提供的主动管理和监控来推进下一个企业计划，针对复杂的 Microsoft 挑战寻找下一个解决方案，并积极主动地应对下一个威胁。Quest Software。Where Next Meets Now. 有关详细信息，请访问：www.quest.com。

如果您对可能使用的本材料存有任何问题，请联系：www.quest.com/cn-zh/company/contact-us.aspx