

2010年7月28日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

【報道資料】

**メディア・アラート：チェック・ポイントのリサーチ・チーム、ToolTalk データベース・サーバに
深刻な脆弱性を発見**

**チェック・ポイントの IPS ソリューション、ToolTalk データベース・サーバのパーサに発見された脆弱性
および、先頃修正パッチが公開された Microsoft 製品のゼロデイ脆弱性に対応**

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社(本社:東京都新宿区、代表:代表取締役社長 杉山隆弘)は本日、当社のIPSリサーチ・チームが先頃、ToolTalkデータベース・サーバのパーサに深刻な脆弱性を発見したと発表しました。この脆弱性が悪用された場合、問題のあるシステムにリモートから任意のコードを送り込まれ、実行されるおそれがあります。チェック・ポイントの[IPS Software Blade](http://www.checkpoint.com/defense/advisories/public/announcement/2010/071410-tooltalk-db-server-vulnerability.html)およびNGX SmartDefenseは、不正な細工が施されたデータベース・リクエストを検出して遮断できるため、これらの製品とサービスをご利用のお客様は本脆弱性の影響を受けません。ToolTalkデータベース・サーバの脆弱性と対応する保護機能の詳細については、<http://www.checkpoint.com/defense/advisories/public/announcement/2010/071410-tooltalk-db-server-vulnerability.html>をご覧ください。

今回確認された脆弱性は、データベース・ファイルの作成と管理を行うRPCベースのToolTalkデータベース・サーバに存在し、IBM AIXバージョン6.1.3以前、Sun Solaris 10 Sparc/x86以前、HP HP-UX 11.0以前を使用しているすべてのシステム・ユーザに影響します。この脆弱性は、チェック・ポイントのIPSリサーチ・チームが発見し、責任を持ってベンダー各社に情報を提供しました。同チームは、攻撃者らに悪用される可能性がある未知の脆弱性を発見するため、ネットワークやプロトコル、アプリケーションの脆弱性に関する独自の調査を行っています。チェック・ポイントでは、ベンダーが提供する最新の修正パッチを適用すると共にIPSを最新の状態にアップデートし、直ちにこの脆弱性に対応することを推奨しています。

またチェック・ポイントは併せて、当社のIPS Software BladeとNGX SmartDefenseソリューションは、先頃Microsoftより修正パッチが公開された次の2つのゼロデイ脆弱性(問題発覚時にパッチが公開されていなかった脆弱性)に対応していると発表しました。

- [Windowsのヘルプとサポート・センター\(HSC\)の脆弱性](#) – 攻撃者はこの脆弱性を利用して、不正な細工が施されたHTMLファイルをInternet Explorerで開かせ、リモートから任意のコードを実行することができます。
- [Canonical Display Driverの脆弱性](#) – 攻撃者はこの深刻な脆弱性を悪用し、特別な細工が施された画像ファイルを、問題のあるアプリケーションで開かせようとしています。

チェック・ポイントの IPS ソリューションが提供する侵入防御機能は、当社のゲートウェイ製品に統合されており、これらの脆弱性を悪用する攻撃を検出して遮断します。チェック・ポイントの IPS 製品は当社のアップデート・サービスによって強化され、各種のアップデートや、防御機能およびセキュリティ・ポリシーの設定アドバイザーがリアルタイムかつ継続的に提供されます。これらの防御機能は、世界各地のセキュリティ・リサーチ & レスポンス・センターが開発、提供しています。

Software Blade アーキテクチャをベースとする IPS Software Blade は、マルチギガビットの速度で動作し、クライアントやサーバ、OS の各種脆弱性、マルウェアやワームへの感染などの多種多様な脅威に対し事前対応的な防御を提供する、総合的な次世代ファイアウォール侵入防御機能です。Software Blade は相互に独立した柔軟なセキュリティ・モジュールであり、これらを組み合わせることで自社の要件に最適なセキュリティ・ゲートウェイを構築することができます。

これらの脆弱性とチェック・ポイントが提供する保護機能の詳細については、
<http://www.checkpoint.co.jp/defense/advisories/public/index.html>をご覧ください。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド(www.checkpoint.com)は、インターネット・セキュリティにおけるトップ企業として、特にネットワーク、データ、およびエンドポイントのトータル・セキュリティを単一の統合管理フレームワークで提供できる唯一のベンダーとして広く認められています。チェック・ポイントは、セキュリティの複雑さと総所有コスト(TCO)を低減しつつ、あらゆるタイプの脅威からお客様のネットワーク環境を確実に保護するための妥協のないセキュリティ機能を実現しています。チェック・ポイントは、FireWall-1 と特許技術のステートフル・インスペクションを開発した業界のパイオニアです。チェック・ポイントは、革新的セキュリティ技術である Software Blade アーキテクチャのさらなる開発と発展に努めています。Software Blade アーキテクチャは、導入先にあわせカスタマイズすることで、あらゆる組織、あらゆる環境のセキュリティ・ニーズにも的確でダイナミックに対応できる、安全かつ柔軟でシンプルなソリューションの構築を可能にします。チェック・ポイントは、Fortune 100 社の全社を含む、何万ものあらゆる規模の企業や組織を顧客としています。数々の受賞歴のあるチェック・ポイントの ZoneAlarm ソリューションは、世界中で何百万にも及ぶお客様の PC をハッカー、スパイウェア、および情報窃盗から未然に保護しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社は、1997年10月1日設立、東京都新宿区に拠点を置き、36名の従業員を擁しています。

#####

©2003-2010 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, Check Point のロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, puresecurity の logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, totalsecurity のロゴ, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone

Labs, Zone Labs のロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書に記載された製品は米国の特許 No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および 7,165,076 により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

担当 マーケティング担当 溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501

Email: info_jp@checkpoint.com

広報代行 株式会社プラップジャパン

担当 落合

Tel: 03-4570-3191/ Fax: 03-4570-3189