

2009年11月27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 IPS ソリューションと Endpoint Security、
Microsoft Internet Explorer に発見された新たなパッチ未公開の脆弱性から企業を保護
Internet Explorer 6 および 7 に見つかったゼロデイ攻撃を受ける脆弱性に対応**

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、セキュリティ・ゲートウェイである Check Point R70、VPN-1® R65、VPN-1 VSX R65、InterSpect®、IPS 製品、および Endpoint Security WebCheck が、先ごろ Microsoft Internet Explorer (IE) に見つかった、修正パッチがマイクロソフト社より公開されていない脆弱性に対する保護を提供できると発表しました。この脆弱性が悪用された場合、IE がクラッシュし、システムが攻撃を受けやすい状態に陥ります。チェック・ポイントの上記製品をご使用の場合は、対応する修正パッチを適用することなく、この脆弱性から PC を保護できます。

このパッチ未公開の脆弱性は「Summoner」(「召喚人」の意)とも呼ばれ、削除済みのオブジェクトに IE がアクセスしようとしたときに問題が発生します(これは「死者からの召喚」と呼ばれます)。この状態を引き起こすため、攻撃者は、IE を異常終了させる不正な Web ページを作成する可能性があります。IE がこの方法で異常終了させられた場合、システムは脆弱な状態に陥り、攻撃者はそのシステム上で任意のコードを実行できるようになります。この脆弱性の影響を受けるのは、Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Microsoft Windows 2000 SP4 で動作する IE6 と IE7 です。IE6 と IE7 は、現在も広く使用されています。

チェック・ポイントの IPS ソリューションと Check Point Endpoint Security は、この脆弱性を悪用しようとする HTML ページを検知してブロックします。Check Point R70 の IPS Software Blade、VPN-1 R65、VPN-1 VSX R65、InterSpect、および Endpoint Security WebCheck は、対応する修正パッチをネットワーク中のクライアント PC に適用することなく、この脆弱性から PC を保護できます。この脆弱性からネットワークを保護するために、利用しているチェック・ポイント製品のアップデートを行う必要はありません。本メディア・アラートの執筆時点では、Microsoft からの修正パッチはまだ未提供となっています。チェック・ポイントは、この脆弱性を悪用する攻撃を防御できる事前対応型の保護機能を 2006 年 11 月より提供しています。

侵入防御機能を提供するチェック・ポイントの IPS ソリューションは、専用プラットフォームまたは統合ゲートウェイで使用することができ、チェック・ポイントの各種サービスを通じて継続的にアップデートされます。チェック・ポイントは、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リをリアル

タイムに提供しています。チェック・ポイントの防御機能は、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する包括的なインライン型侵入防御ソリューションで、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といった幅広い脅威に対する事前対応型の防御機能を提供します。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。チェック・ポイントの IPS 製品の詳細については、

<http://www.checkpoint.co.jp/products/softwareblades/intrusion-prevention-system.html>

をご覧ください。

Check Point Endpoint Security WebCheckは、パッチ未公開の脆弱性や、ドライブバイ・ダウンロード(マルウェアの自動ダウンロード攻撃)といったWebベースの脅威からエンドユーザのPCを保護します。WebCheckが備える特許出願中の仮想化技術は、Web攻撃を「サンドボックス」にリダイレクトして封じ込めることによって、オペレーティング・システムへの被害を防ぎます。Check Point WebCheckの詳細については、www.checkpoint.co.jp/products/webcheck/index.htmlをご覧ください。

今回発見された脆弱性およびチェック・ポイントが提供する保護機能の詳細については、<http://www.checkpoint.com/defense/advisories/public/2009/cpai-24-Nov.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。2009 年には、新たな革新的セキュリティ技術として Software Blade アーキテクチャを開発しました。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、約33名の従業員を擁しています。

#####

©2003-2009 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 Cl, 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。本書で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 佐藤

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