Jeff Jones Security Blog
http://blogs.technet.com/security
Japan Security Team Blog
http://blogs.technet.com/jpsecurity
2008/1/15

WINDOWS VISTA

1 年間の脆弱性レポート

Jeffrey R. Jones 著
Security Guy
(Microsoft Director)

CSS Japan Security Response Team 訳
(マイクロソフト株式会社)

© 2007, Jeffrey R. Jones, All Rights Reserved

目次

概要 2

著者の紹介 4

概要 5

分析結果の解釈 5

セキュリティ研究者のエコシステム 6

Windows Vista 対 Windows XP 8

Windows Vista の 1 年間 8

Windows XP の 1 年間 11

対比 14

Winodws VISTA 対そのほかのオペレーティング システム 16

Red Hat Enterprise Linux 16

Ubuntu 6.06 LTS 19

Apple Mac OS X v10.4 22

比較検討 23

最後に 25

付録 A よくある質問 27

付録 B: ソースおよび方法論 31

未解決の脆弱性の発見 32

概要

Windows Vista のビジネス利用のお客様向けの出荷が 2006 年 11 月でしたので、2007 年 11 月末で、このサポートされた製品が広く使用されて 1 年になります。

このレポートでは Windows Vista 1 年目までに公開された脆弱性とセキュリティ更新プログラムの分析をし、従来の Windows XP やその他の最新のワークステーション OS システムである Red Hat や Ubuntu、アップル製品などとも関連させて考察しています。

分析の結果、Windows Vista は従来の製品に比べてセキュリティの脆弱性の点で改善されています。セキュリティ更新プログラムの分析からもまた、従来の Windows XP と比べて、マイクロソフトがセキュリティ更新プログラムや開発のプロセスを改善したことで、Windows の管理者の皆様のセキュリティ更新の手間が著しく軽減しているということがわかります。

このレポートは以前に公開した「Windows Vista 90 日間の脆弱性レポート」(英語情報) と「Windows Vista 6 ヶ月間の脆弱性レポート」(英語情報) に続く最新のレポートです。1 年という期間でさらに多くの情報収集ができ、このレポートにはより詳しい分析結果が含まれています。

© 2007, Jeffrey R. Jones, All Rights Reserved

© 2007, Jeffrey R. Jones, All Rights Reserved

著者の紹介

Jeff Jones はマイクロソフトの信頼できるコンピューティング (Trustworthy Computing) グループのセキュリティ戦略担当重役です。その立場で、20 年間にわたるセキュリティ関連の経験を生かして企業の最高セキュリティ責任者の皆様やマイクロソフト内のセキュリティ チームとともにマイクロソフトの製品づくりやそのプロセスに実用的で測定可能なセキュリティの向上を推進しています。マイクロソフトで戦略的なこの役職につく以前、Jeff は Network Associates 社でセキュリティ関連の製品管理を担当する VP でした。そこで Jeff は、PGP、Guantlet、Cybercop などの製品を担当し、McAfee 製品の改善にも携わりました。これらのポジションは 20 年間のセキュリティ関連のキャリアの最高峰であり、リスク評価や、カスタム ファイアー ウォールの構築、Trusted Information Systems の一員として DARPA セキュリティ リサーチのプロジェクトにも携わりました。

Jeff は読者に自分の仮説や分析、結論などを鵜呑みにして、裏付けもなく盲目的に支持されるよりも、批判的なフィードバックをすることを熱心に勧めており、同時にその批判的なフィードバックをサポートするものとして自分と同じかそれ以上に高い水準の方法論や分析を求めるのです。

© Copyright 2007, Jeffrey R. Jones, All rights reserved.

概要

これは Windows Vista が出荷されてから私が書いた 3 つ目の脆弱性分析レポートのです。最初の 2 つは 90 日間のレポート (9o day report) (英語情報)と 6 ヶ月間のレポート (six month report) (英語情報)でした。

このレポートでは、より詳細な分析内容を反映するためにすこし構成を変えました。このレポートは大きく分けて 2 つのセクションからなります。

- Windows XP 従来機種である Windows XP と Windows Vista との比較
- Windows Vista と他の Windows を提供しているその他の OS との比較

分析結果の解釈

この分析レポートに何が含まれており、なぜある人たちの役に立つ可能性があるのか、そしてたぶん一番大事なことは、何をカバーしていないかについて少しここでふれておく必要があるのではないかと思います。

セキュリティというものを一つのものさしで測れるものなら、あらゆる要素、例えばソフトウエアの質、管理のためのコントロール、物理的なコントロール、など多くの要素だけでなく、それ以外の要素も含めて複雑な組み合わせを総合して測らなければならないだろうと思います。仮にそれができたとしても、そのコンピュータなりシステムなりのために作られたセキュリティ ポリシーとの兼ね合いも考慮に入れなくてはなりません。

つまり、このレポートは「セキュリティ」の分析ではないのです。ここにあげる製品のセキュリティ機能を考察して、なぜより確かなプライバシー管理ができるとか、ビジネスのプロセスを安全に守るかを検討したものでもありません。まして、ここで検討している製品でセキュリティポリシーの管理がどれほど楽にできるか考察したりなどしていません。

この分析レポートで、あるソフトウエアが他よりも安全性に優れていることを証明するのでしょうか。いいえ、それは私の意図ではありません。

このレポートは脆弱性の分析で、もっと広い意味でのセキュリティ分析の一部とみなせる要素もあるかもしれません。基本的に私はセキュリティ関連の機能もセキュリティと関連のない機能も、意図した通りに機能し、誤った使い方をしてセキュリティの問題にならないためには、しっかり

© Copyright 2007, Jeffrey R. Jones, All rights reserved.

としたエンジニアリングとゆるぎないセキュリティ品質という基盤の上に構築されていなければならないと思っています。

では数量の観点から見ることに意味があるのでしょうか。ひとつの要素で絶対的な「セキュリティ」のレベルを測ることはできないということは認めながら、それでもその要素を見ることでセキュリティを改善したり、リスク マネージメントを今より容易にすることには役立つと思うのです。

- 他の条件がすべて同じ場合、 1 年間に 10 の脆弱性の問題がある場合と、100 ある場合とどちらがコンピュータ上のリスクを対応するのが楽でしょうか。
- みなさんのセキュリティ チームとそのリスク管理のプロセスにとって、 1 年に 10 のセキュリティ更新プログラムを適用すると 100 のそれをするのではどちらのほうが悪影響が大きいでしょうか。

指標はそれぞれ互いに排他的であることもあるということは知っておいてください。どういうことかというと、販売側がポリシーで 1 年に 1 度のセキュリティ更新を義務づけている場合、セキュリティ パッチの数は絶対的に減るでしょう。しかし、このポリシーのために、問題が公開されてから対処されるまでの時間は長くなります。

私が脆弱性分析というとき、ユーザーのリスクを減らすということを目標にして、脆弱性のレベルを測定しています。

セキュリティ研究者のエコシステム

分析に入る前に、すこしセキュリティ研究者のエコシステムとソフトウエア内の弱点を探知する科学についてみてみましょう。最近刊行されたマイクロソフト セキュリティ インテリジェンス レポートによると、2001 年にはたった 1528 件だった脆弱性が、2007 年には 3400 件以上見つかっています。

これは セキュリティ研究者の業界が成長、成熟し、ソフトウエアの脆弱性探知に熟達してきたことを暗示する兆候の 1 つです。近年ではツールも著しく向上してきて、プロ用だったコードのスキャニング ツールのなかには製品としてリリースされたものもいくつかありますし、Fuzz テストのような新しい技術も開発され、ソフトウエア セキュリティの限界を押し上げる傾向にあります。

© 2007, Jeffrey R. Jones, All Rights Reserved

2001 年と比べたら今日の新しい OS ははるかに厳しい精査の目に晒されています。数字をあげることはできませんが、私の意見では、はるかに多くの研究者がいるうえ、彼らのレベルも上がっているし、かつてないほどの高度なツールとテクニックも持っているようで、セキュリティの脆弱性をより見つけやすい環境になっています。

© 2007, Jeffrey R. Jones, All Rights Reserved

WINDOWS VISTA 対 WINDOWS XP

Windows XP の後継として Windows Vista は 2006 年 11 月 30 日にビジネス ユーザー向けにリリースされました。2001 年の Windows XP のリリース以来、マイクロソフトはセキュリティに対して、著しい変化を経験しました。2002 年 1 月には Windows XP のリリースからほんの数ヶ月後でありながら、マイクロソフトは信頼できるコンピューティングという構想を立ち上げて、お客様に長期的で継続的なセキュリティの改善をゴールに全製品の開発プロセスを改定し始めました。

この構想に基づくことで Windows Vista のセキュリティに関して新しい Windows 製品の脆弱性を減らすという観点から、どれだけの効果があったでしょう。実績は継続的にモニターし続けなくてはなりませんが、2007 年 11 月 30 日で、Windows Vista ビジネス カスタマー向けに完全に提供開始してから 1 年になります。改善の様子を検討し始めるのに十分な時間がたっていると思います。

WINDOWS VISTA の 1 年間

初期の脆弱性の兆候の全体像を見るのに、 1 年間で Windows Vista 用に出されたアドバイザリ、更新プログラム、脆弱性への対処 (セキュリティ更新プログラム)、および脆弱性の公開についてみてみましょう。

この 1 年間の Windows Vista 用のセキュリティ更新プログラムについてまず見てみましょう。マイクロソフトは １７ のセキュリティ情報とそれに対応する Windows Vista の影響を受けるコンポーネントについてセキュリティ更新プログラムをリリースし、1 年に Windows Vista のセキュリティ更新プログラムがリリースされた日を集約すると、 9 日ありました。

更新プログラムがひとつでもリリースされた場合、パッチ イベントと呼んで、日数を単位としています。セキュリティ更新プログラムの日数と頻度からコードのセキュリティのレベルはわかりませんが、更新プログラムがリリースされて、その適用性を査定し、展開戦略を決めるために集まるセキュリティ チームにとっては興味のあることかもしれません。

さらに、セキュリティ更新プログラムごとに対応した脆弱性を抜き出してみました。Windows Vista に関して初年度にマイクロソフトは合計 ３６ の脆弱性を対処し、セキュリティ更新プロ

© 2007, Jeffrey R. Jones, All Rights Reserved

グラムは 9 日間ありました。Table はセキュリティ情報、脆弱性の識別名とベンダーにとってセキュリティ更新プログラムごとの深刻度評価をまとめてあります。

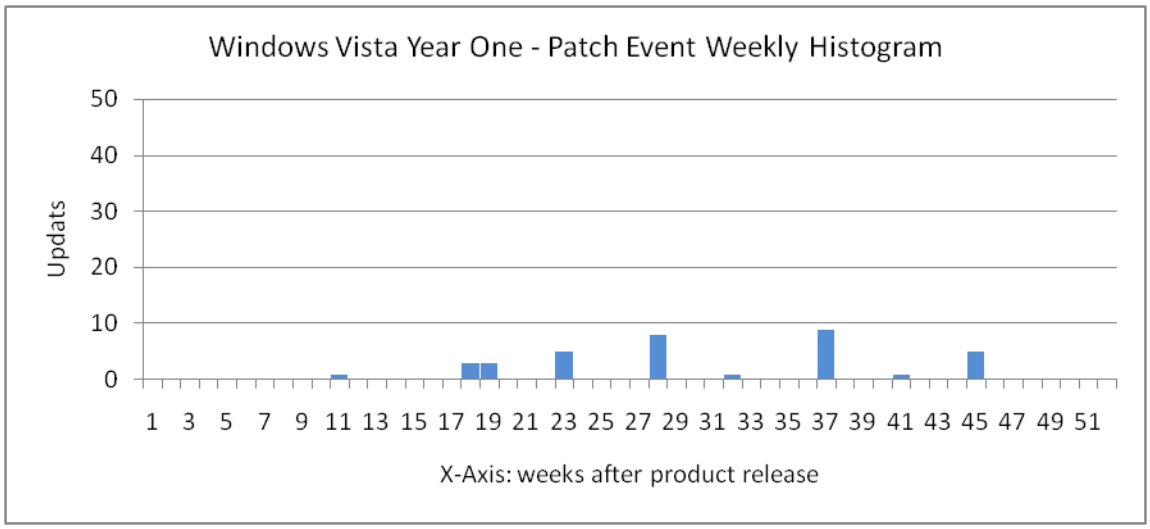
日付	セキュリティ情報	脆弱性	コンポーネント	深刻度評価
2/13/2007	MS07-010	CVE-2006-5270	ウイルス対策エンジン	緊急 (Critical)
4/3/2007	MS07-017	CVE-2007-1212 CVE-2007-0038 CVE-2007-1215	EMF, Animated cursor, GDI	重要 (Important) 緊急 (Critical) 重要 (Important)
4/10/2007	MS07-021	CVE-2006-6696 CVE-2007-1209 CVE-2006-6797	CSRSS	緊急 (Critical) 重要 (Important) 注意 (Low)
5/8/2007	MS07-027	CVE-2007-0942 CVE-2007-0945 CVE-2007-0946 CVE-2007-0947 CVE-2007-2221	IE	重要 (Important) 緊急 (Critical) 重要 (Important) 重要 (Important) 緊急 (Critical)
6/12/2007	MS07-032 MS07-033 MS07-034	CVE-2007-2229 CVE-2007-2222 CVE-2007-1751 CVE-2007-1499 CVE-2007-2227 CVE-2007-2225 CVE-2007-1658 CVE-2006-2111	User info. Store, IE, Windows Mail, User info. Store、IE、Windows Mail	警告 (Moderate) 緊急 (Critical) 緊急 (Critical) 警告 (Moderate) 警告 (Moderate) 重要 (Important) 緊急 (Critical) 重要 (Important)
7/10/2007	MS07-038	CVE-2007-3038	Windows Firewall	警告 (Moderate)
8/14/2007	MS07-042 MS07-045	CVE-2007-2223 CVE-2007-3041	XML Core, IE, WMP,	緊急 (Critical) 重要 (Important)

© 2007, Jeffrey R. Jones, All Rights Reserved

	MS07-047 MS07-048 MS07-050	CVE-2007-2216 CVE-2007-3891 CVE-2007-3033 CVE-2007-3032 CVE-2007-1749	Gadgets, VML	重要 (Important) 警告 (Moderate) 重要 (Important) 警告 (Moderate) 緊急 (Critical)
9/11/2007	MS07-053	CVE-2007-3036	Subsystem for UNIX	重要 (Important)
10/9/2007	MS07-056 MS07-057 MS07-058	CVE-2007-3897 CVE-2007-3893 CVE-2007-3892 CVE-2007-1091 CVE-2007-2228	Windows Mail, IE, RPC	重要 (Important) 緊急 (Critical) 警告 (Moderate) 注意 (Low) 重要 (Important)

Table： Windows Vista 用のセキュリティ更新プログラムの詳細

この 1 年間セキュリティ更新の頻度と管理者への影響を見やすくするために、リリースから 52 週間のセキュリティ更新プログラムの日数をグラフにしてみました。



Figure： Windows Vista 1 年間のパッチ イベントの週単位の集計図

さらに、前のセクションで概要を述べた脆弱性対策に加えて、Windows Vista では初年度に未解決の 30 の脆弱性が公開されました。

© 2007, Jeffrey R. Jones, All Rights Reserved

WINDOWS XP の 1 年間

次に、マイクロソフトが信頼できるコンピューティングという構想を立ち上げる以前の 2001 年 10 月 25 日に出荷になった Windows XP について同じようにみてみましょう。

マイクロソフトは Windows XP を出荷した初めの 1 年間に 30 のセキュリティ情報とその影響を受ける Windows XP のための更新プログラムをリリースしました。さらに、2001 年のマイクロソフトは更新プログラムのリリースを管理者が予想できる様に月例で公開する方針に切り替えていませんから、30 のセキュリティ情報を 1 年間のうち 26 日にわたってリリースしています。

個々のセキュリティ更新日ごとに脆弱性を抜き出してみると、マイクロソフトは Windows XP に関してその初年度に合計 65 の脆弱性を解決していることがわかります。Table はその詳細です。

日付	セキュリティ情報	脆弱性	コンポーネント	深刻度評価
10/21/2001	MS01-051	CVE-2001-0664 CVE-2001-0665 CVE-2001-0667	IE	深刻度評価 システム導入以前
11/1/2001	MS01-054	CVE-2001-0721	Plug-n-play	注意 (Low)
11/8/2001	MS01-055	CVE-2001-0722 CVE-2001-0723 CVE-2001-0724	IE	緊急 (Critical)
11/20/2001	MS01-056	CVE-2001-0719	Windows Media Player	緊急 (Critical)
12/13/2001	MS01-058	CVE-2001-0727 CVE-2001-0874 CVE-2001-0875	IE	緊急 (Critical)
12/20/2001	MS01-059	CVE-2001-0876 CVE-2001-0877	Plug-n-play	緊急 (Critical)
2/11/2002	MS02-005	CVE-2002-0022	IE	緊急 (Critical)

© 2007, Jeffrey R. Jones, All Rights Reserved

		CVE-2002-0023 CVE-2002-0024 CVE-2002-0025 CVE-2002-0026 CVE-2002-0027		
2/12/2002	MS02-006	CVE-2002-0053	snmp	警告 (Moderate)
2/21/2002	MS02-008 MS02-009	CVE-2002-0057 CVE-2002-0052	XML core, IE	緊急 (Critical) 緊急 (Critical)
2/27/2002	MS02-012	CVE-2002-0055	SMTP	注意 (Low)
3/4/2002	MS02-013	CVE-2002-0058 CVE-2002-0076	MS jvm	緊急 (Critical)
3/28/2002	MS02-015	CVE-2002-0077 CVE-2002-0078	IE	緊急 (Critical)
4/4/2002	MS02-017	CVE-2002-0151	UNC	警告 (Moderate)
4/10/2002	MS02-018	CVE-2002-0072 CVE-2002-0073 CVE-2002-0074 CVE-2002-0075 CVE-2002-0147 CVE-2002-0148 CVE-2002-0149 CVE-2002-0150	IIS	緊急 (Critical)
5/15/2002	MS02-023	CVE-2002-0188 CVE-2002-0189 CVE-2002-0190 CVE-2002-0191 CVE-2002-0193 CVE-2002-1564	IE	緊急 (Critical)
6/11/2002	MS02-029	CVE-2002-0366	RAS	緊急 (Critical)
6/26/2002	MS02-032	CVE-2002-0372	Windows Media Player	緊急 (Critical)
7/30/2002	MS02-040	CVE-2002-0695	MDAC	緊急 (Critical)

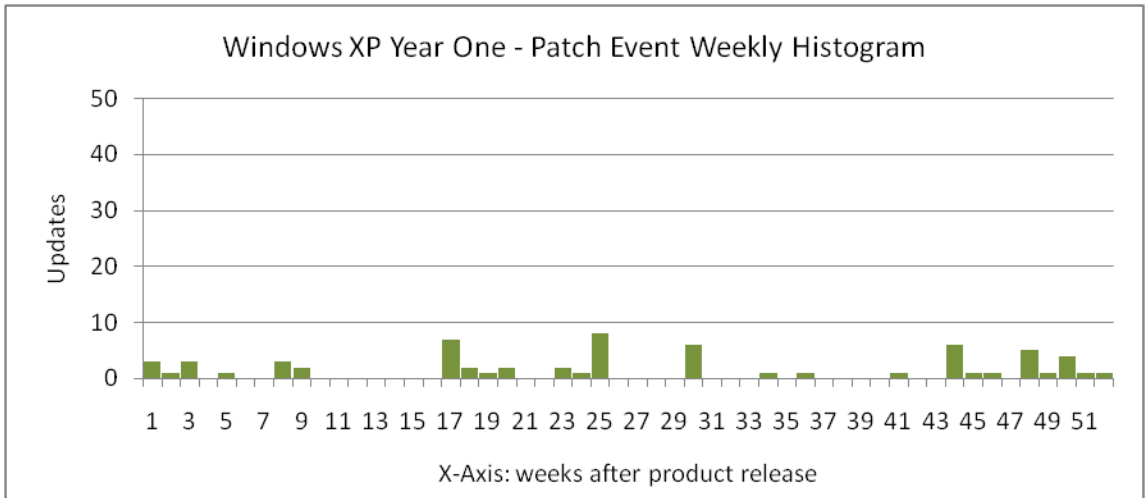
© 2007, Jeffrey R. Jones, All Rights Reserved

8/21/2002	MS02-045 MS02-047	CVE-2002-0724 CVE-2002-0371 CVE-2002-0647 CVE-2002-0648 CVE-2002-0722 CVE-2002-0723	SMB, IE	警告 (Moderate) 緊急 (Critical)
8/28/2002	MS02-048	CVE-2002-0699	Cert enrollment	緊急 (Critical)
9/4/2002	MS02-050	CVE-2002-0862	Cert validation	重要 (Important)
9/18/2002	MS02-051 MS02-052	CVE-2002-0863 CVE-2002-0864 CVE-2002-0865 CVE-2002-0866 CVE-2002-0867	RDP, MS jvm	警告 (Moderate) 緊急 (Critical)
9/24/2002	MS02-053	CVE-2002-0692	Frontpage Server Extensions	緊急 (Critical)
10/3/2002	MS02-054 MS02-055	CVE-2002-0370 CVE-2002-1139 CVE-2002-0693 CVE-2002-0694	Zip decompression, Windows help	警告 (Moderate) 緊急 (Critical)
10/10/2002	MS02-058	CVE-2002-1179	OE, IE	緊急 (Critical)
10/16/2002	MS02-060	CVE-2002-0974	Help	警告 (Moderate)

Table： 1 年間に公開された Windows XP 用のセキュリティ情報と脆弱性

Windows XP の初年度がセキュリティ管理者にとってどんなだったかパッチ イベントごとの図である Figure でよくわかります。

© 2007, Jeffrey R. Jones, All Rights Reserved

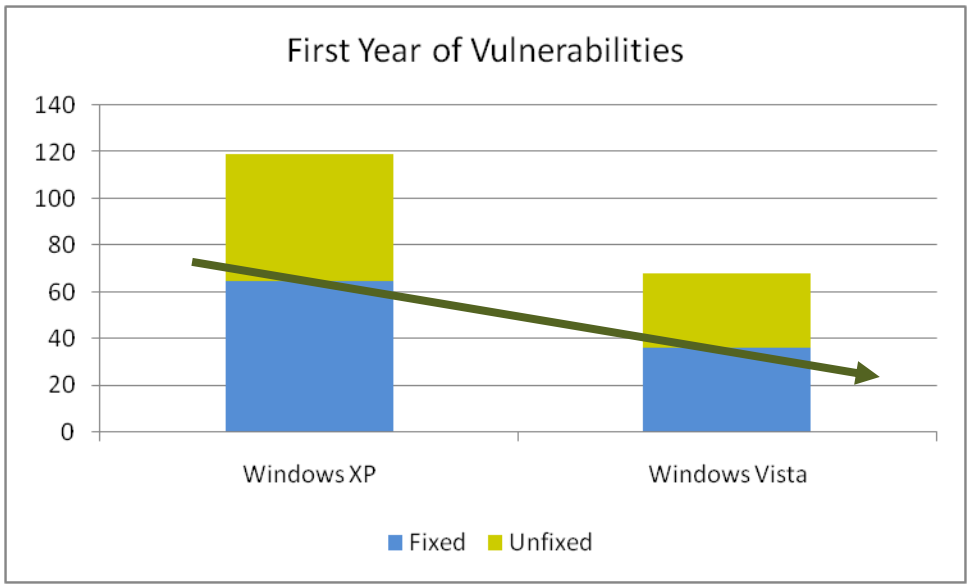


Figure： Windows XP 1 年間のパッチ イベントの週単位の集計図

さらに、前のセクションで概要を述べた Windows XP 用の脆弱性対策に加えて、Windows XP の初年度には未解決の 54 の脆弱性が公開されました。

対比

Windows Vista と Windows XP に関して基本的な分析が済みましたので比較する情報は十分です。まず、解決済みと未解決の脆弱性の表を並べて見てみましょう。

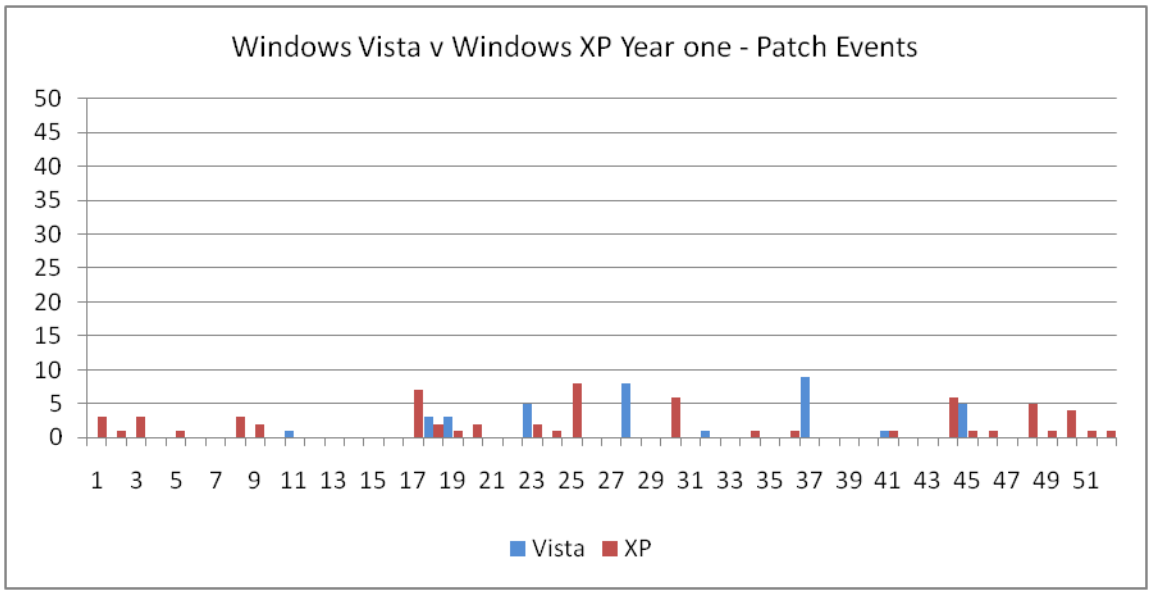


Figure：初年度の脆弱性の比較 Windows Vista 対 Windows XP

© 2007, Jeffrey R. Jones, All Rights Reserved

Figure からセキュリティ研究者が見つけた脆弱性の数が Windows XP に比べて Windows Vista で著しく減ったことは明らかです。

次に Figure でパッチ イベントを比較して管理者へのセキュリティ更新プログラムの影響を見てみましょう。Windows vista は 1 年間に 17 のセキュリティ更新プログラムが、それぞれ別の週の 9 日にわたってありました。Windows XP では 30 のセキュリティ更新が 26 日にわたってあり、それが週単位では 25 週にわたっています。



Figure： Windows Vista 対 Windows パッチ イベントの比較図

こうやってグラフにしてみると、Widows XP について 2001 年から 2002 年にかけてと Windows Vista の 2007 年と比べてみて、管理者が予測しやすい月例公開方式とセキュリティ更新の減少によりセキュリティのリスク管理に要する仕事量を大きく削減することができたことがよくわかります。新しいプロセスを取り入れたことで、お客さまが更新のスケジュールを事前に知ることができると同時に、お客さまの仕事量を増やす重要な脆弱性の数を減らすという、マイクロソフトが信頼できるコンピューティングという構想で時間をかけて向上したことをよくあらわしています。Windows XP SP2 をお使いのお客様にとっても、またこの月例のセキュリティ更新スケジュールが役に立っていることでしょうし、Windows Vista をお使いのお客様は時間がたつにつれさらにこの利点を実感されるはずです。以下はここまでお話ししてきた内容の主なデータをまとめたものです。

測定基準	Windows Vista (1 年目)	Windows XP (1 年目)

© 2007, Jeffrey R. Jones, All Rights Reserved

解決済の脆弱性	36	65
セキュリティ更新プログラム	17	30
パッチ イベント	9	26
パッチ イベントが最低 1 日あった週	9	25

Figure： Windows Vista と Windows XP の比較のまとめ

WINODWS VISTA 対そのほかのオペレーティング システム

Windows ユーザーのためのセキュリティの向上が、私が検証を行っている重要な目標ですが、Windows Vista がそのほかの既存のオペレーティング システムとどのように比較されるかを調査することもまた興味深いです。この目的のため、私は長期的なサポート オプションを提供するそのほかのワークステーション製品 (Red Hat、Ubuntu および Mac OS X 10) を見てみることにしました。これらの各々について、私は少なくともリリースされてから 1 年間経っている最新のバージョンのオペレーティング システムをテストしました。

RED HAT ENTERPRISE LINUX

Red Hat は最も一般的な Enterprise Linux ディストリビューションで、このため、1 年間利用可能となっているこれらの最新のサポートされたリリースである Red Hat Enterprise Linux 4[1] Workstation (rhel4ws) を私は最初にテストします[2]。

- 2005 年 2 月 15 日に rhel4ws が 出荷された時、一般に利用可能となる前に、既に出荷されるコンポーネントに存在する脆弱性が 129 件公開されていました。出荷日に Red Hat はこれらの脆弱性のうち 64 件を解決するための 27 件のセキュリティ アドバイザリを公開しました。

---

[1] Red Hat は 2007 年 3 月 Red Hat Enterprise Linux 5 を出荷しました。これは 1 年間たっていないので含まれていません。

[2]この情報の主なソースは http://rhn.redhat.com/errata です。

© 2007, Jeffrey R. Jones, All Rights Reserved

- 利用可能となってから最初の 1 年間で、Red Hat は rhel4ws についての 183 件のセキュリティ アドバイザリ/更新プログラムを公開しました。深刻度が Critical および Important である問題に限定すると、57 日にわたり 88 件公開されました。
- 利用可能となってから最初の 1 年間で、Red Hat は合計で 493 件の rhel4ws に存在する脆弱性を修正しました。Critical または Important とされている脆弱性に限定すると、修正された脆弱性の件数は 214 件です。
- 最初の年の終わりには 82 件の脆弱性が、修正プログラムのない状態で公開されました。(これは後に異なる修正プログラムおよびセキュリティ アドバイザリで修正されるでしょう。) これを修正された脆弱性に加えると、最初の年に総計 575 件の脆弱性が RHEL4 のコンポーネントで確認されたことになります。

もちろん、Red Hat Enterprise Linux 4 WS として Red Hat が出荷し、サポートしている製品のコンポーネントのすべてについての脆弱性を数えるのは「公平」ではないという考え方もあります。(しかし、私は Windows XP に対し IIS Web Server の脆弱性を数えました。この理由は Windows XP にはこのコンポーネントが同梱されていたためです。) この考えをふまえ、比較すると、私はさらに Windows XP と同様の機能性を提供する rhel4ws のコンポーネットと、そのほかのオプションのコンポーネントを除外した縮小セットを分析しました。私は比較にこのコンポーネントの縮小セットのみを使用します。

RHEL4WS – 縮小コンポーネントのセット

Red Hat およびそのほかの Linux ディストリビューションベンダーは Microsoft Windows オペレーティング システム上の比較の対象となりうるコンポーネントを持たない多くのアプリケーションを含め、サポートすることにより、自分たちのワークステーション ディストリビューションに価値を加えます。Linux ディストリビューションに対し「オプションの」アプリケーションを考慮するのは公平ではないということは Windows と Linux の比較に対する一般的な反論であるため、私は Windows OS に同梱されている機能と比較可能ではないコンポーネントの脆弱性は除外し、さらに分析しました。つまり、私は rhel4ws コンピュータをインストールし、次を行いました。

- 既定でインストールされていないコンポーネントは除外しました。これは rhel4ws に同梱されているすべてのオプションの「サーバー」コンポーネントを含みます。

© 2007, Jeffrey R. Jones, All Rights Reserved

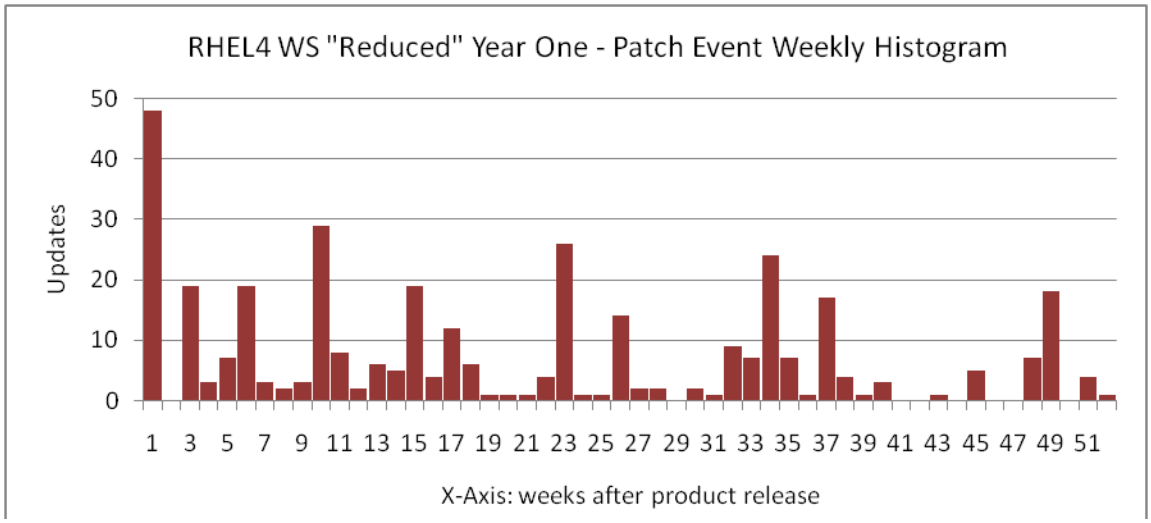
- さらに、テキスト インターネット、グラフィックス (Gimp のものです) およびオフィス (OpenOffice) および開発ツール (gcc など) のインストール グループを除外しました。
- rpm コマンドを使用して、インストールされているすべてのパッケージの一覧を作成し、そのパッケージの一覧を使用し、脆弱性が含まれないようにフィルタしました。

このプロセスにより、標準のシステム管理ツール、ブラウジングのための Firefox、音声およびビデオのサポートは含みますが、penOffice および既定で Windows システムが持たないその他のオプションと、全てのサーバー パッケージを除外した Gnome-windows ワークステーションを作りました。この縮小された rhel4ws のビルドを比較のために検証しました。

- 最初の 1 年間で、Red Hat は 64 日にわたりコンポーネントの rhel4ws の縮小セットに影響をおよぼす 125 件のセキュリティ アドバイザリを公開しました。Red Hat により Critical または Important と評価された問題を含むセキュリティ アドバイザリのみに限定すると、30 週間の 41 日で 62 件のアドバイザリが公開されました。
- Red Hat はコンポーネントの縮小された「ワークステーション」 rhel4ws のセットに影響を及ぼす 360 件の脆弱性を修正しました。Red Hat により Critical または Important と評価されたもののみに限定すると、脆弱性の件数は 154 件でした。
- この 1 年間の終わりで、コンポーネントの縮小セットに存在する公開された脆弱性の 40 件は Red Hat から修正プログラムがまだ提供されていませんでした。

rhel4ws の縮小コンポーネント セットにとって、フル プロダクトよりも良い 1 年間となりましたが、Red Hat のお客様は縮小インストールでさえも、かなり多くの脆弱性およびセキュリティ更新プログラムに直面していました。

© 2007, Jeffrey R. Jones, All Rights Reserved



Figure： RHEL4WS の「縮小された」1 年間 – パッチ イベントの週毎のグラフ

このグラフで、私はパッチ イベントを図表にするにあたり週毎の分析を使用しました。このため、各々のパッチ イベントが示されているわけではありません。Red Hat のケースでは、数週間は実際に複数のパッチ イベントがありました。Figure で見られるように、縮小された rhel4ws の最初の年でパッチ イベントがなかったのはわずか 8 週のみです。

UBUNTU 6.06 LTS

次は Ubuntu 6.06 LTS の比較です。Ubuntu は多くの人に最も一般的で前途有望な Linux ディストリビューションであると考えられており、2006 年 6 月 1 日にリリースされた Ubuntu 6.06 バージョン[3]の長期的なサポート (LTS) が約束されていました。長期的なサポートは多くの企業内での使用のために、ディストリビューションにとって重要な要件であると考えられているため、Ubuntu にとってサポートの約束は戦略的なものとなっています。

- Ubuntu 6.06 LTS は 2006 年 6 月 1 日の利用可能となった日以前に既に 53 件[4]の公開された脆弱性がありました。

---

[3] これはまた Ubuntu 6.10, 7.04 またはそれ以降を分析しない理由もでもあることに注意してください。今までのところ Ubuntu は長期的なサポートを 6.06 のみに約束しており、それ以降のリリースには長期的なサポートを行っていません。

[4] この数字は 6 か月間の報告で確認した数字よりも若干高いことに注意してください。これは、マイクロソフト以外の製品に使用している方法論がベンダーにより確認され、修正された脆弱性のみを数えるためで、このため、

© 2007, Jeffrey R. Jones, All Rights Reserved

- 最初の年、Ubuntu は Ubuntu 6.06 LTS についての 181 件のセキュリティ アドバイザリを公開しました。修正はパッチ イベントは集約してもその年の 119 日発生しました。
- 修正プログラムで Ubuntu は Ubuntu 6.06 LTS に影響を及ぼす 406 件の脆弱性に対処しました。これらの修正された脆弱性のうち 160 件は NVD で深刻度 High と評価されました。
- 1 年間の終わりで、Ubuntu 6.06 LTS に存在する一般に公開された脆弱性の少なくとも 55 件がまだ Ubuntu から修正プログラムが提供されていませんでした。これを対処された 406 件に加えると、合計で 461 件の脆弱性となります。

Ubuntu のお客様にとっては Red Hat のお客様よりも若干よい最初の年となったようです。Ubuntu 6.06 は rhel4ws の 16 か月後に出荷されたことを考えれば、Red Hat およびそのほかのベンダーのオープン ソースの貢献から恩恵を得たのかもしれません。

UBUNTU 6.06 LTS – 縮小コンポーネント セット

RHEL4WS に行ったコンポーネント セットの縮小のように、私は Ubuntu 6.06 LTS に追加の分析を行い、Windows OS に同梱される比較の対象となる機能を持たないコンポーネントの脆弱性を除外しました。

- Ubuntu は実際はインストール時にコンポーネントの選択という観点ではフレキシビリティを提供しません。そのかわり、Ubuntu はデスクトップおよびサーバーのインストール用に別途インストール CD を提供します。私は Ubuntu 「デスクトップ」の iso をダウンロードし、デスクトップ インストール ディスクを作成しました。
- インストールを実行し、その後 'dpkg –list' を使用しインストールされたパッケージの一覧を生成しました。「オプションのサーバー」のパッケージはまったく存在せず、これはサーバーのインストールに存在する可能性があるためであろうことに気付きました。
- 私は手動で gimp および OpenOffice をパッケージの一覧から除外しました。そのほかは除外しませんでしたが、これはほとんどのユーザーが既定のデスクトップのインストールから手動でパッケージを削除することはないだろうと思ったためです。

修正する時期は各ベンダーにより異なります。この理由をよりよく理解するためには、"Estimating Software Vulnerabilities," IEEE Security & Privacy, vol. 5, no. 4, 2007, pp. 28-32 をご覧ください。

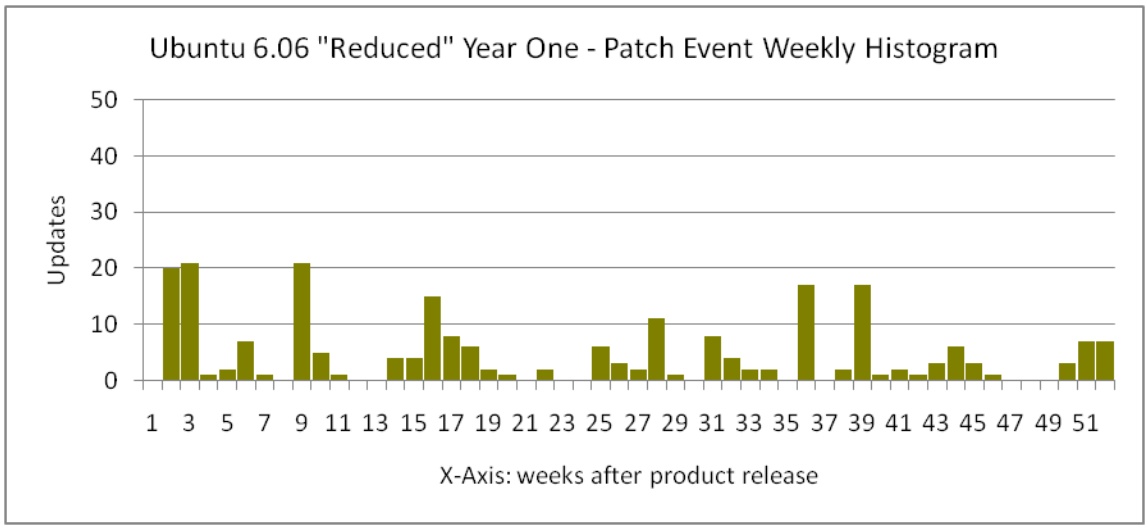
© 2007, Jeffrey R. Jones, All Rights Reserved

- 私は結果のパッケージの一覧を使用して存在していなかったパッケージ内の脆弱性をフィルタしました。

基本的にこの結果は、標準のシステム管理ツール、ブラウジングのための Firefox、音声およびビデオのサポートは含みますが、OpenOffice および既定で Windows コンピュータが持たないその他のオプションと、全てのサーバー パッケージを除外した Gnome-windows ワークステーションを作りました。この縮小された Ubuntu のビルドが比較のために検証されました。

- 利用可能となってから最初の 1 年間で、Ubuntu は Ubuntu 6.06 の縮小デスクトップビルドに対応する 80 件のセキュリティ アドバイザリを公開しました。修正プログラムはその年の 39 週間のうち 65 日公開されました。
- 最初の 1 年間で、Ubuntu はコンポーネントの縮小された Ubuntu のデスクトップ セットに影響を及ぼす 224 件の脆弱性を修正しました。
- その期間の終わりで、コンポーネントの縮小セットに存在する一般に公開された 18 件の脆弱性は Ubuntu からまだ修正プログラムが提供されていませんでした。

また、標準のデスクトップのインストールを使用している Ubuntu のお客様について、Red Hat RHEL4WS のユーザーよりも発生する脆弱性の件数が少ないことが確認されました。しかし、パッチ イベントという観点ではその差異はほとんどなく、Red Hat は 64 件で Ubuntu は 65 件でした。



Figure： Ubuntu 6.06 の縮小の 1 年目 – パッチ イベントの週毎のグラフ

© 2007, Jeffrey R. Jones, All Rights Reserved

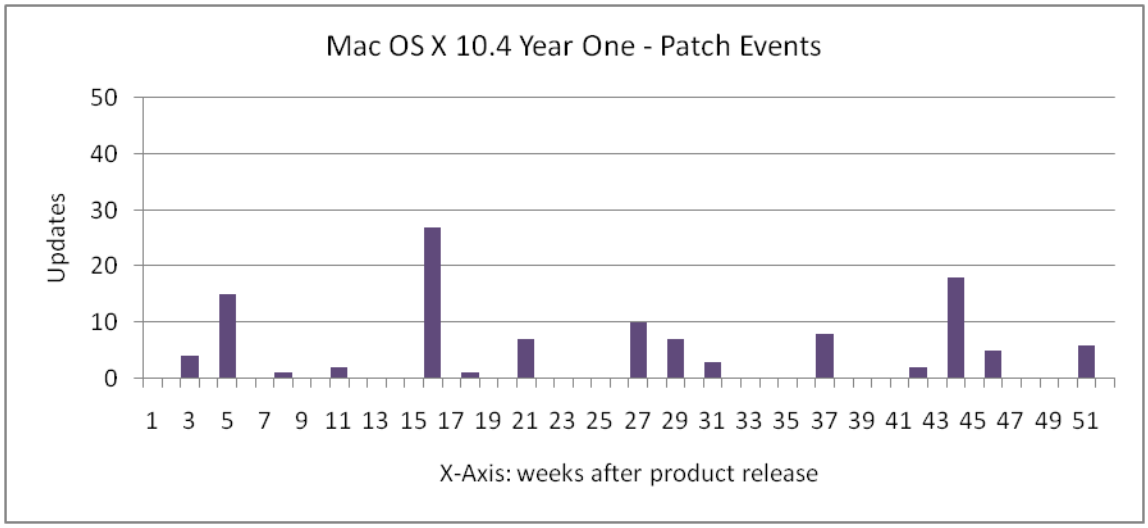
Ubuntu 6.06 LTS にパッチ イベントがなかったのは 1 年のうち 13 週のみで、このため少なくとも 1 件のセキュリティ更新プログラムがその年の週の 75% でリリースされていました。

APPLE MAC OS X V10.4

Apple[5] は Mac OS X 10.4 を 2005 年 4 月 29 日に出荷しました。

- 最初の年、Apple は Mac OS X 10.4 に影響を及ぼす 17 件のセキュリティ更新プログラムをそれぞれ異なる日に公開しました。
- これらの更新プログラムは Mac OS X 10.4 の出荷されているコンポーネントに存在する 116 件の脆弱性を修正しました。
- 1 年間の終わりで、製品に存在する一般に公開された 41 件の脆弱性が Apple から修正プログラムが提供されていませんでした。このため、この製品について修正済みおよび未修正のものを含め公開された脆弱性の総数は 157 件でした。

以下は Mac OS X 10.4 の最初のパッチ イベントのグラフです。



Figure： Mac OS X 10.4 1 年目 – パッチ イベント

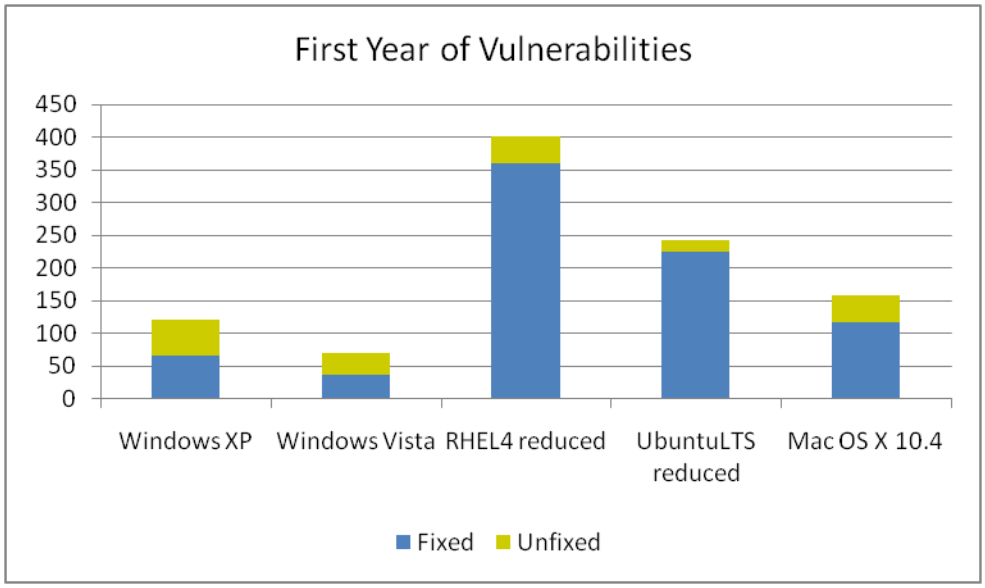
[5] Apple は 2007 年 10 月 26 日に Leopard を出荷しました。これはまだ 1 年間たっていないため、含まれません。

© 2007, Jeffrey R. Jones, All Rights Reserved

1 年間の 15 週で 17 件のパッチ イベントが発生しており、そのうち 2 週が更新プログラムが公開された日が 1 日以上あります。

比較検討

Windows Vista と他の業界の製品との基本的な個別の比較が済んだので、比較する情報が十分になったと思います。まず、解決されたのと未解決の脆弱性を図にして比較してみましょう。

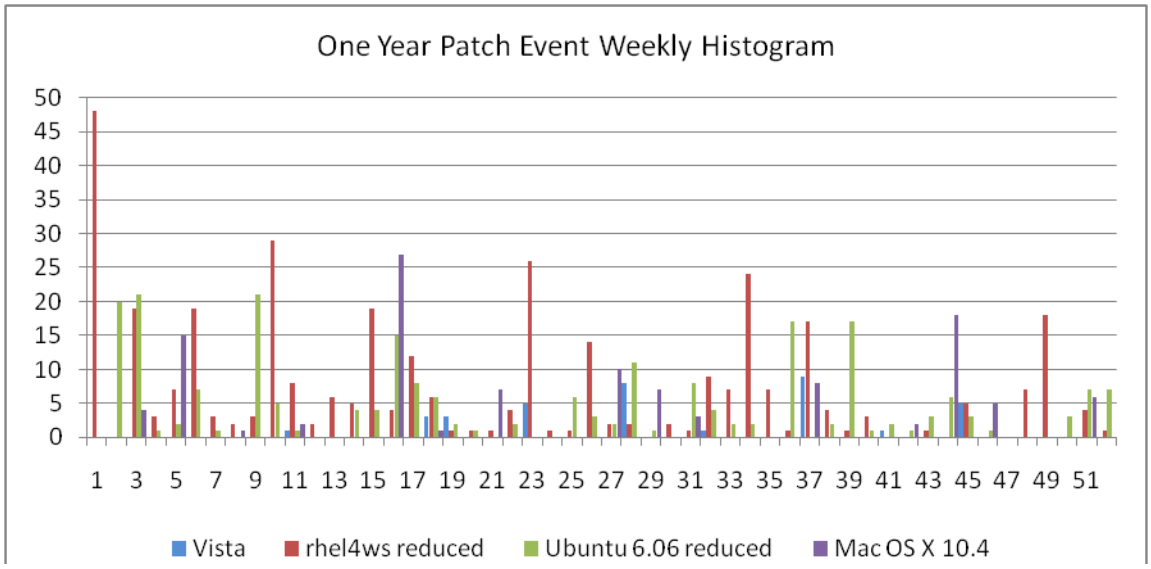


Figure： Windows Vista と他の OS 製品の 1 年目の脆弱性の比較

Figure から Windows Vista のセキュリティの脆弱性の減少は従来の製品と比べてだけでなくそのほかの業界の OS が提供しているものと比べてもはるかに少ないことがわかります。

次にセキュリティ更新プログラムが管理者にあたえる影響をパッチ イベントで見てみましょう。Windows Vista の １７ のセキュリティ更新プログラムは 9 日間のパッチ イベントで 1 年で 9 週間にわたってありました。ほかの OS のパッチ イベントがあった週比較した図にしてみました。

© 2007, Jeffrey R. Jones, All Rights Reserved



Figure： Windows Vista 対他の業界の OS での パッチ イベントの比較

この場合はグラフにして視覚的に見てもわかりずらいので、下の Table で少し比較しやすくしてみました。

指標	Windows Vista (1 年目)	Windows XP (1 年目)	Red Hat rhel4ws reduced (1 年目)	Ubuntu 6.06 LTS reduced (1 年目)	Mac OS X 10.4 (1 年目)
解決済の脆弱性	36	65	360	224	116
セキュリティ更新プログラム	17	30	125	80	17
パッチ イベント	9	26	64	65	17
パッチ イベントが少なくとも 1 日あった週	9	25	44	39	15

Table： 分析した全製品の要約

© 2007, Jeffrey R. Jones, All Rights Reserved

表からわかるように、また Windows Vista がほかの OS よりも成績が良く、脆弱性の数もより少なく、セキュリティ管理者への影響が潜在的にあるセキュリティ更新プログラムのある週も少ないです。

最後に

Windows Vista 初年度のセキュリティに関して良い点も悪い点もいろいろなことが言われたり書いたりしています。このレポートでは、いくつかの測定可能な要素を秩序立てて考察してみようとしました。それらの要素はもっと広い意味でのセキュリティの一部でもありえますし、セキュリティの脆弱性とその更新プログラムの観点からどれほどの改善がなされたかという点で Windows Vista が意味するものを理解していただけたかもしれません。

製品のリリース後 1 年間に研究者が見つけて公開した脆弱性を研究してきました。これは製品のリリース以前に、個々のベンダーがセキュリティの脆弱性を発見し、解決することを開発過程でどれだけ効果的にやっているかを知るための研究の 1 指標です。私の分析では、研究者が発見して公開した脆弱性の数は 従来の Windows XP や、Red Hat Enterprise の Linux, Ubuntu や Apple の Mac OS X 10.4 など他の OS 比べて Windows Vista で著しく減っています。

さらに少なくとも更新プログラムが 1 つでもある日をパッチ イベントとして、週単位で図にしました。パッチ イベントは、製品のセキュリティの質とベンダーの更新プログラムのリリースの方針と方法との組み合わせがどのようにセキュリティ管理者に影響をあたえるか、特に、セキュリティ更新プログラムを 1 つ以上展開する必要があるのかを判断するために 1 年間に何日くらい管理者が駆り出されたかという形で影響を測る間接的な指標です。私が分析してわかったのは、管理者のみなさんが駆り出されなければならない頻度は比較検討した他の製品よりも Windows Vista のほうがはるかに少ないということです。

最後に、もう 1 度繰り返して言いたいのは、セキュリティの質（脆弱性の減少に反映されるように）は製品のセキュリティに重要不可欠な部分だと思っていますが、それでもこれはセキュリティの全体像のほんの 1 部分に過ぎません。もしも皆さんがこのレポートをセキュリティ全体の査定努力の一部として使うなら、さらに以下を検討するよう強くお勧めします。

- 個々のビジネス プランの応じたセキュリティの性能。たとえば、BitLocker ドライブ暗号化はラップトップのポリシーには有益な機能である場合も多いでしょう。

© 2007, Jeffrey R. Jones, All Rights Reserved

- 深層での守りを提供することができるような設計上および保守的なセキュリティ機能。Windows Vista を含む最新の製品はファイアウォール、スタック プロテクションやライブラリのランダム化などの進んだ機能を実装しています。
- 皆さんのポリシーに適した管理のしやすさ。ポリシーの変更を集中管理の立場から容易にできるでしょうか。ポートのロックを包括的にできるでしょうか。証明書を包括的に承認することはどうでしょう。みなさんのコンピュータ使用環境がポリシーに準拠しているかの確認はどうでしょう。単純な構成上のエラーが大きなセキュリティ上の問題になりかねません。管理が容易であるというのは考慮すべき大切な点です。

© 2007, Jeffrey R. Jones, All Rights Reserved

付録 A よくある質問

初めて読む人から質問が出てブログでコメントしたりメールで答えていることを今までこの種の分析やレポートでの経験で知っています。そういう人のためにすこし先回りしてありそうな質問も含めてこのレポートで答えておくことにしましょう。

Q:　マイクロソフトで働いている人の言っていることなんてどうして信じられると思うのですか。

ほかによくあるパターンは、「マイクロソフトの得にならない結果でも公開できたと思うんですか。」 です。

私はいつでもこの質問が好きなのだというと、みなさん驚きます。本当のところは悪い結果が出るなどという心配はしていないのです。もっといい質問はなぜそれほど結果に自信を持ってこのプロジェクトを始められたか、かもしれません。

考えても見てください。マイクロソフトはもう 6 年にもわたって製品のセキュリティの改善にかなりの投資をしてきています。セキュリティについてのコミットメントは本物です。この会社に入る前に私自身もできるかぎその点を確証のあるものとしました。誰が信じようと信じまいと、私はこの会社に 5 年いて、経営陣のコミットメントとひたむきな努力をまのあたりに見ています。そして Mike Howard や David Cross のような素晴らしいセキュリティ関連の人たちと一緒に働いてこられたことをうれしく思っています。チームが大きくなり、James Whittaker や、最近では Vinny Gullotto など、この業界の専門家たちをも引き寄せてきたのを見てきているのです。

だからこそ、いつもそうするように言えるのです。なんでも鵜呑みにしないでください。みなさんが自分で見つけたいと思うなら、私は 「かき回しているのだ」 と思ってください。みなさんが,どんどん疑問を持って、なぜ結果がそうなったかのか突っ込んで考えてもらうこと、それが私の究極的なゴールなのです。誰でもこのレポートの分析と同じ手順を踏むことができるように、私のレポートの出典はに掲載してあります。新発見について話し合うのを楽しみにしています。

Q: 2006 年から 2007 年の 11 月 30 日から 11 月 30 日までのようにではなく、各製品の 1 年目と比較したのは何故ですか。

© 2007, Jeffrey R. Jones, All Rights Reserved

私は製品が市場に出てから最初の 12 か月を対象にリサーチをしました。新製品を評価し、どのような利点がこの製品の開発手法に見られるか検討できるからです。一定の期間を選んで個々の製品を評価すると、製品によってはすでに何年か市場にでているものもあり（安定期を過ぎている可能性さえある）、開発のプロセスに戻って報告された脆弱性を査証するのが困難になるでしょう。Window XP と Windows Vista は製品開発の過程がまったく異なっています。Windows XP はセキュリティ開発ライフサイクルの開発以前にリリースされているからです。

興味のある方は、2007 年という枠組みでの比較もしますので
http://blogs.technet.com/security に分析が出るのを楽しみにしていてください。

Q: Linux ディストリビューションには Windows よりもはるかに多くのアプリケーションのオプションが含まれています。つまり統一性がないわけですけれどそういう比較がどうして有効だといえるのでしょう。

実のところ Windows Vista と Windows XP でもコンポーネントが違います。Windows Vista Ultimate はたとえば Media Center が入っていますが、Windows XP Professional には含まれていません。ユーザーの立場からは、統一性のある比較だと思います。どの OS を選ぼうと、大抵の人は規定のコンポーネントをインストールして、それを使っていると思います。脆弱性がそういうコンポーネントに含まれているとすれば、その危険にさらされ、緩和策をとる必要がでてきます。

しかし Linux ディストリビューションのオプションのコンポーネントを除外したり、比較対象が明らかに存在しないコンポーネントは規定のものでも除外するなどしてできる限りの地ならしをしたつもりです。その逆に、Windows の分析には製品に含まれているコンポーネントはすべて含めました。ですから比較は有効で有益だと思っています。

Q: いわゆる 「サイレント フィックス」 はどうですか？過去のあなたの分析はマイクロソフトが内部で発見してひそかに修正した問題が数に含まれていないので比較は無意味だと批判されています。

これは興味深い考え方です。確かにどのベンダーの製品であれ、記録されてなければ、セキュリティ上の問題が解決されていても私にはわかりません。公に検討されたことでなければ知りえないわけです。

たとえば、アップルの品質保証チームが Leopard のリリース中にいくつセキュリティの脆弱性を見つけてただ修正しただけなのか知りません。さらに、どれだけのバグが見つかって、それが

© 2007, Jeffrey R. Jones, All Rights Reserved

見つかっていなかったら、セキュリティ上の問題になっていたかもしれないということをチームのメンバーでさえ誰も気づかずに直したのかも知りません。Linux ディストリビューションについても同様です。rhel4 Update 5 の開発過程で修正されたバグのうちどれだけがセキュリティ上の問題になる可能性があったのか知る由もありません。

脆弱性の数を数え上げるという意味では、サイレント フィックスが起こることもあるということを示す例をいくつかあげることができます。CVE-2007-5959 を例にとってみましょう。脆弱性の識別番号は 1 つですが、その定義は 「不特定複数の脆弱性」 です。私の分析ではこれを 1 つと数えています。なぜなら CVE 識別番号が 1 つだからです。同様に、CVE-2004-1057 は 「Linux カーネル上の複数のドライバ」 が適切にメモリを記録せず、サービス拒否を有効にするとあります。技術的には複数の脆弱性がひそかに修正されるわけですが、どの分析でもこれを私は 1 つとしか数えません。これらの製品は複数の問題がどの分析にも詳述されないという恩恵を被っています。

その反面、マイクロソフトのセキュリティ更新プログラムには MSRC ポリシーとして、内部で発見された脆弱性がリスク査定を変更する場合、外部で発見された脆弱性と同等の深刻度がある場合や回避策や緩和策が適用にならない場合は記録として残すことになっています。ですからその製品について公開された問題を数えることで、みなさんのリスクを増やす脆弱性の識別可能なものを使用しているといえるでしょう。

もっと一般的には、理論上の 「サイレント フィックス」 がどの製品についてでも実際に簡単に見つかるものなら、そしてどのベンダーの製品でもそうなら、公開された脆弱性に当然加えられて、測定することもできるわけです。

究極的には、いわゆるサイレントフィックスに対する批判は少し、公開された脆弱性の分析の核となる結果からみなさんの気をそらすためのもののように思えます。

Q: (脅威にさらされるまでの) 猶予日数を含まなかったはなぜですか。

私は(脅威にさらされるまでの) 猶予日数は、テストや対応の早さなど、公開された脆弱性に対するベンダーの対応の 1 部である要素の組み合わせを計測するのに重要な指標だと思っています。しかしそれと同時にマイクロソフトが Vista に関して 2007 年にどうだったかを、2005 年の Red Hat や 2006 年の Ubuntu と比べることに価値があるとは思えません。

© 2007, Jeffrey R. Jones, All Rights Reserved

もっと興味深い質問は、この 1 年間にそれぞれどうだったかでしょう。同様に、別の分析レポートを、2007 年にベンダーごとの (脅威にさらされるまでの) 猶予日数について仕上げる予定ですので興味のあるかたは http://blogs.technet.com/security での分析結果を楽しみにしていてください。

© 2007, Jeffrey R. Jones, All Rights Reserved

付録 B: ソースおよび方法論

Mitre Corporation 率いる共同体が Common Vulnerabilities and Exposure (CVE) リストを公開して、複数の脆弱性のデータベースとセキュリティ製品に活用できるような共通の命名ルールを公開し始める以前は脆弱性を識別して修正するのに共通の命名ルールがありませんでした。CVE の命名法とそのプロセスは世界中のあらゆるソフトウエア製品にわたる脆弱性を包括的なリストとして成功しています。このレポートでも個々の脆弱性を識別するのに CVE 命名法を使用しています。

このレポート内の分析はインターネット上で入手可能なデータソースを複数使用して集め、カスタマイズし、照合されたデータを使用しています。

- http://www.microsoft.com/technet/security/current.aspx で公開のマイクロソフトセキュリティ情報とその関連サイト
- https://rhn.redhat.com/errata/rhel4ws-errata-security.html で公開の Red Hat セキュリティアドバイザリとその関連サイト
- http://www.ubuntu.com/usn で公開の Ubuntu セキュリティ 通知とその関連サイト
- Mitre CVE リスト (http://cve.mitre.org) のデータベースの上位集合である National Vulnerability Database (NVD)。NVD はまた米国国土安全保障省も後援しており、XML のフォーマットでデータを http://nvd.nist.gov/download.cfm からダウンロードすることもできます。
- 脆弱性の詳細の検証や特に最初に公開された日を確認するのに多くのセキュリティ関連サイトを使いました。もっとも頻繁に使用したサイトは、www.securityfocus.com、Bugtraq のメールリスト、www.secunia.com や www.securitytracker.com などがありますが、ほかにも多数ありました。

これらやその他の情報源を利用して分析した製品の脆弱性のデータベースを集めました。未解決の脆弱性を集めることに関しては 「未解決の脆弱性の発見」 と題したセクションにさらに多くの詳細を載せてあります。

このレポートで 「公開」 と言っているのは広く一般に公開することで、個人的とか一定の人にだけの公開を意味するものではありません。

© 2007, Jeffrey R. Jones, All Rights Reserved

未解決の脆弱性の発見

6 ヶ月間の分析レポート公開後、未解決の脆弱性の割合について多くのコメントを受けましたので、すこしはっきりさせて、なぜ見解に差が生じたのかの詳細を述べておいたほうがいいかと思います。このレポートでは、基本的に公開された脆弱性で未解決のものを発見して数えるのに 2 つの方法を用いています。

方法 1 ：個別の詳細な研究。このレポートの Windows Vista と Windows XP に使用した方法です。本質的にその製品の脆弱性に関して初年度の末までに公開されていて、私の解決済のリストに含まれていないものを NVD やその他の情報源で細かくチェックしました。この方法の利点は潜在的に正確性が高いことです。欠点は時間がかかるということと、ほとんどの Linux ベースの OS のようなディストリビューションを断定的に一目で理解するのが難しいということです。

> **例**： *Firefox 1.0.*と出荷された *rhel4ws* の場合。*Firefox 1.0* については *NVD* で *12* 個の脆弱性を識別することができました。これらは *Mozilla* のセキュリティ アドバイザリで解決されてはおらず、そのうち *9* 個の脆弱性は *rhel4ws* の *1* 年目末以前に公開されたものです。*rhel4ws* に適用するでしょうか？たぶん、でも私にはわかりません。おそらく *Red Hat* はこれらの問題をテストの段階で出荷以前に解決したのでしょう。ベンダーが後に問題を解決してそれを認めない限り私にはわからないのです。ですから私はこれらを *Red Hat* の未解決の脆弱性には数えませんでした。

方法 2 ：ベンダーが後になって修正したものを識別する方法。Mac OS X と Linux システムに用いた方法です。基本的にはベンダーが確認,修正した全てを網羅したリストを使って、その製品の初年度末までに公開され、初年度末以降になるまで修正されなかったものだけを抜き出しました。この方法の利点が 2 つあります。作業がしやすいことと識別された脆弱性はベンダーが確認したものだということです。

欠点は統計的に有効な時間がたたないと役に立たず、（ですから Windows Vista には全く使用することができませんでした）ベンダーが修正しなかった問題は永久に識別されないということです。

結果として、方法 2 で識別した未解決の脆弱性の数は最小値とみなすべきで、完全なリストと考えるべきではありません。

© 2007, Jeffrey R. Jones, All Rights Reserved

© 2007, Jeffrey R. Jones, All Rights Reserved