国立研究開発法人
情報通信研究機構

プレスリリース
2018年6月11日
国立研究開発法人情報通信研究機構

脆弱性管理プラットフォーム“NIRVANA 改弐”を開発

【ポイント】

- 国産脆弱性スキャナ「Vuls」と連動する脆弱性管理プラットフォーム「NIRVANA 改弐」を開発
- 企業などの組織内で運用中のサーバ機器に対する脆弱性スキャンの結果をリアルタイムに可視化
- 脆弱性対応状況の全体俯瞰や能動的な脆弱性検知を可能にし、組織のセキュリティを向上

国立研究開発法人情報通信研究機構（NICT、理事長：徳田　英幸）サイバーセキュリティ研究室は、国産オープンソースソフトウェア（OSS）の脆弱性スキャナ「Vuls」（バルス）と連動する、脆弱性管理プラットフォーム「NIRVANA 改弐」（ニルヴァーナ・カイ・ニ）を開発しました。

NIRVANA 改弐は、Vuls による組織内のサーバ機器に対する脆弱性スキャンの結果をリアルタイムに可視化することで、脆弱性対応状況の全体俯瞰や脆弱性の詳細情報へのアクセスを容易にします。また、影響範囲の広い脆弱性が公表された場合には、組織内の緊急フルスキャンを行うことで、脆弱性を保有するサーバ機器を能動的に検知できます。これにより、従来高い人的コストを要していた組織内の脆弱性管理が簡便になり、組織のセキュリティ向上が期待できます。

NIRVANA 改弐と Vuls のシステム連携については、2018 年 6 月 13 日（水）～15 日（金）に幕張メッセで開催される「Interop Tokyo 2018」で動態展示を行います。

【背景】

サイバー攻撃の多くは、コンピュータの OS やソフトウェアの情報セキュリティ上の欠陥である「脆弱性」を悪用しています。サイバー攻撃を未然に防ぐためには、企業など組織内の情報システムについて、OS やソフトウェア等の構成を把握し、日々発見・公表される脆弱性への対処を適切に行う「脆弱性管理」が重要です。しかしながら、従来の脆弱性管理は人手に頼る部分が多く、高い人的コストを要するため、組織のセキュリティ向上の障壁になっていました。

図 1 NIRVANA 改弐と Vuls の連動による組織内の緊急フルスキャン

【今回の成果】

NICT はこれまで、サイバー攻撃統合分析プラットフォーム「NIRVANA 改」の研究開発と社会展開を進め、サイバー攻撃発生後のセキュリティ・オペレーションの効率化に取り組んできました。

今回、NICT が開発した脆弱性管理プラットフォーム「NIRVANA 改弐」は、組織内におけるサイバー攻撃発生前の脆弱性管理を効率化するため、フューチャー株式会社（代表取締役会長兼社長 グループ CEO: 金丸 恭文）により開発された国産 OSS 脆弱性スキャナ「Vuls」と連動し、Vuls による組織内のサーバ機器に対する脆弱性スキャンの結果をリアルタイムに可視化します。

NIRVANA 改弐は、組織内におけるサーバ機器の脆弱性対応状況の全体俯瞰（図 2、図 3 参照）を可能にし、検知された脆弱性の詳細情報へのアクセスを容易にします（図 4 参照）。また、影響範囲の広い脆弱性が公表された場合、NIRVANA 改弐のアクチュエーション（自動対処）機能を用いて、組織内で Vuls の緊急フルスキャンを実施することで、脆弱性を保有するサーバ機器を能動的に検知できます（図 1 参照）。

NIRVANA 改弐と Vuls のシステム連携により、組織内の脆弱性管理が簡便になり、組織のセキュリティ向上や人的コストの低減が期待できます。

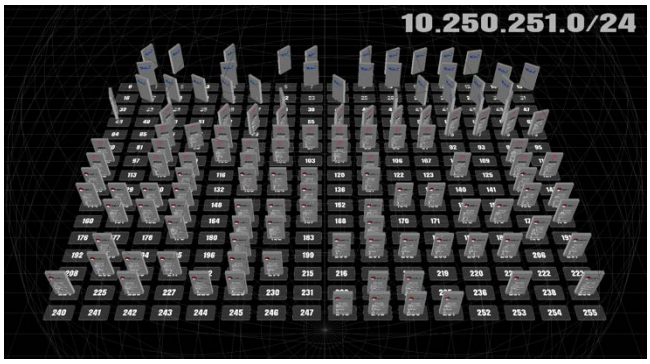

図 2 脆弱性スキャン: 組織内のサーバ機器をモノリスで表現。Vuls で脆弱性スキャン中はモノリスが浮遊

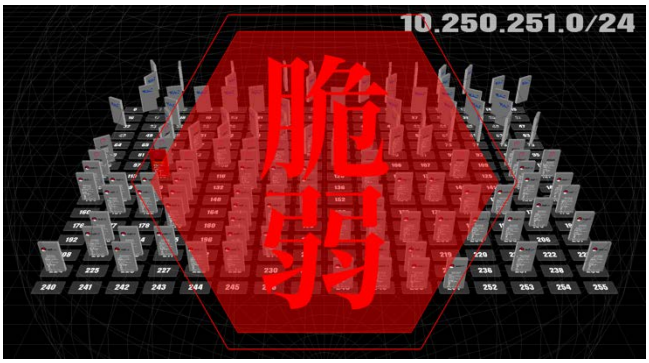

図 3 脆弱性検知: 脆弱性が検知された際は全画面に警告を表示。重大度に応じてモノリスの色が変化

図 4 脆弱性情報表示: モノリス表面に脆弱性の重大度や個数等を表示。詳細情報にもアクセス可能

【今後の展望】

NIRVANA 改弐は脆弱性管理の共通プラットフォームを目指し、Vuls をはじめとする様々な脆弱性スキャナ等との連携を進めていく予定です。NIRVANA 改弐と Vuls のシステム連携については、2018 年 6 月 13 日（水）～15 日（金）に幕張メッセで開催される「Interop Tokyo 2018」で動態展示を行います。https://www.interop.jp/

補足資料

Vuls はエージェントレスの脆弱性スキャナであり、組織内の Linux/FreeBSD 系サーバに SSH（セキュアシェル）経由で定期的に接続し、各サーバの脆弱性スキャンを行います（図 5 参照）。脆弱性スキャンの結果は、NIRVANA 改弐にログメッセージの転送規格である Syslog 形式で送られ、リアルタイムに可視化されます。

Vuls 内部の脆弱性 DB は、米国の NVD（National Vulnerability Database）や日本の JVN（Japan Vulnerability Notes）から脆弱性情報を常時収集し、最新の状態に保たれます。

影響範囲の広い脆弱性が公表された場合には、NIRVANA 改弐のアクチュエーション（自動対処）機能を用いて、Vuls に SSH 経由で緊急フルスキャン命令を送ることができ、Vuls は緊急の脆弱性スキャンを組織内の全サーバに対して行います（図 1 参照）。

万一、組織内のサーバに脆弱性が発見された場合は、NIRVANA 改弐の可視化画面にリアルタイムに警告が表示されます。さらに、NIRVANA 改弐から外部の脆弱性情報にアクセスし、脆弱性の詳細情報を確認することも可能です。オペレータは組織のセキュリティポリシーに従って、サーバのアップデートを行うなど、迅速かつ効率的な脆弱性管理が可能になります。

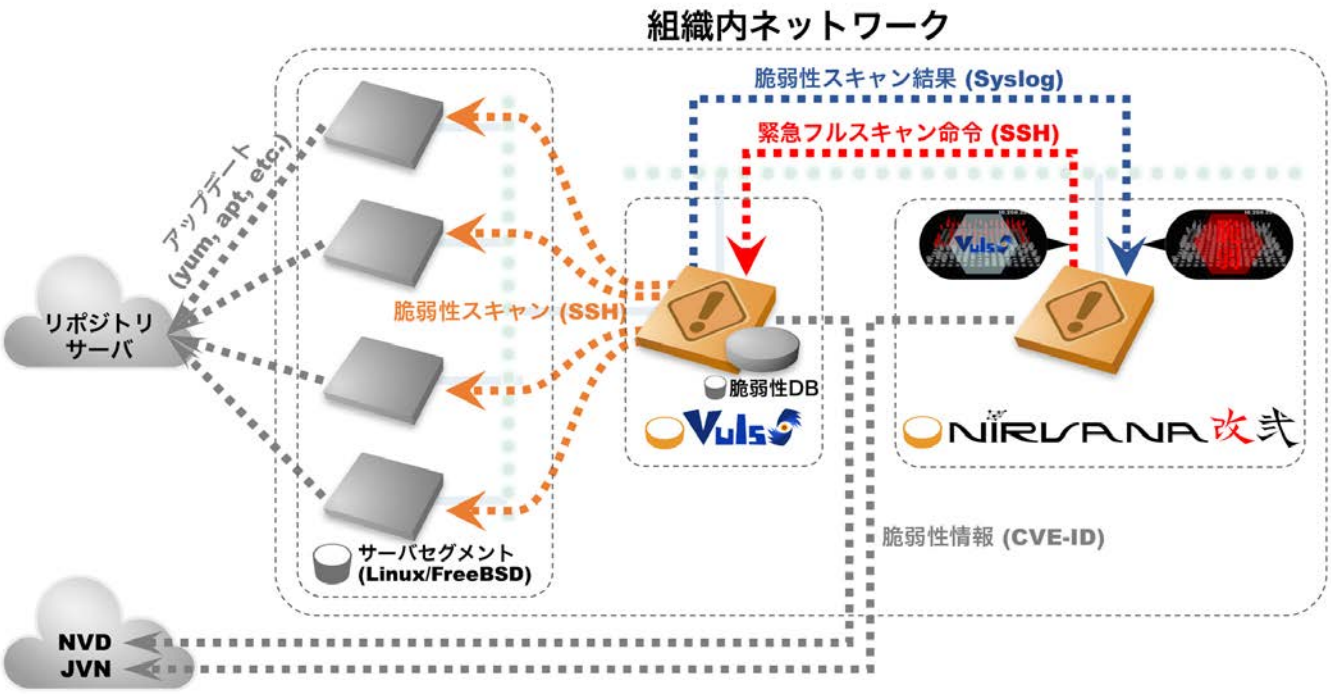

図 5 NIRVANA 改弐と Vuls のシステム連携

＜参考＞

これまでの“NIRVANA 改”関連の報道発表

- 2016 年 6 月 7 日
  「NIRVANA 改が更にバージョンアップ！ ～アラート管理機能の強化と国産機器連携でユーザビリティを大幅向上～」
  http://www.nict.go.jp/press/2016/06/07-1.html

- 2015 年 6 月 8 日
  「サイバー攻撃統合分析プラットフォーム“NIRVANA 改”を機能強化！ ～エンドホスト連携機能と自動防御機能を開発～」
  http://www.nict.go.jp/press/2015/06/08-2.html

- 2013 年 6 月 10 日
  「サイバー攻撃統合分析プラットフォーム“NIRVANA 改”（ニルヴァーナ・カイ）を開発」
  http://www.nict.go.jp/press/2013/06/10-1.html

- 2011 年 6 月 2 日
  「リアルトラフィックの可視化ツール“NIRVANA”を開発 ～通信の「見える化」でネットワーク管理を簡単に～」
  http://www.nict.go.jp/press/2011/06/02-1.html

＜ 本件に関する問い合わせ先 ＞
国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室
井上 大介、鈴木 未央、久保 正樹
Tel: 042-327-6225
E-mail: nicter@ml.nict.go.jp

＜ 広報 ＞
広報部 報道室
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp