

# JVN#8BAAAB4E

## msearch におけるディレクトリトラバーサル脆弱性の脆弱性

受付日

2005/1/17

公表日

2005/3/8

問題

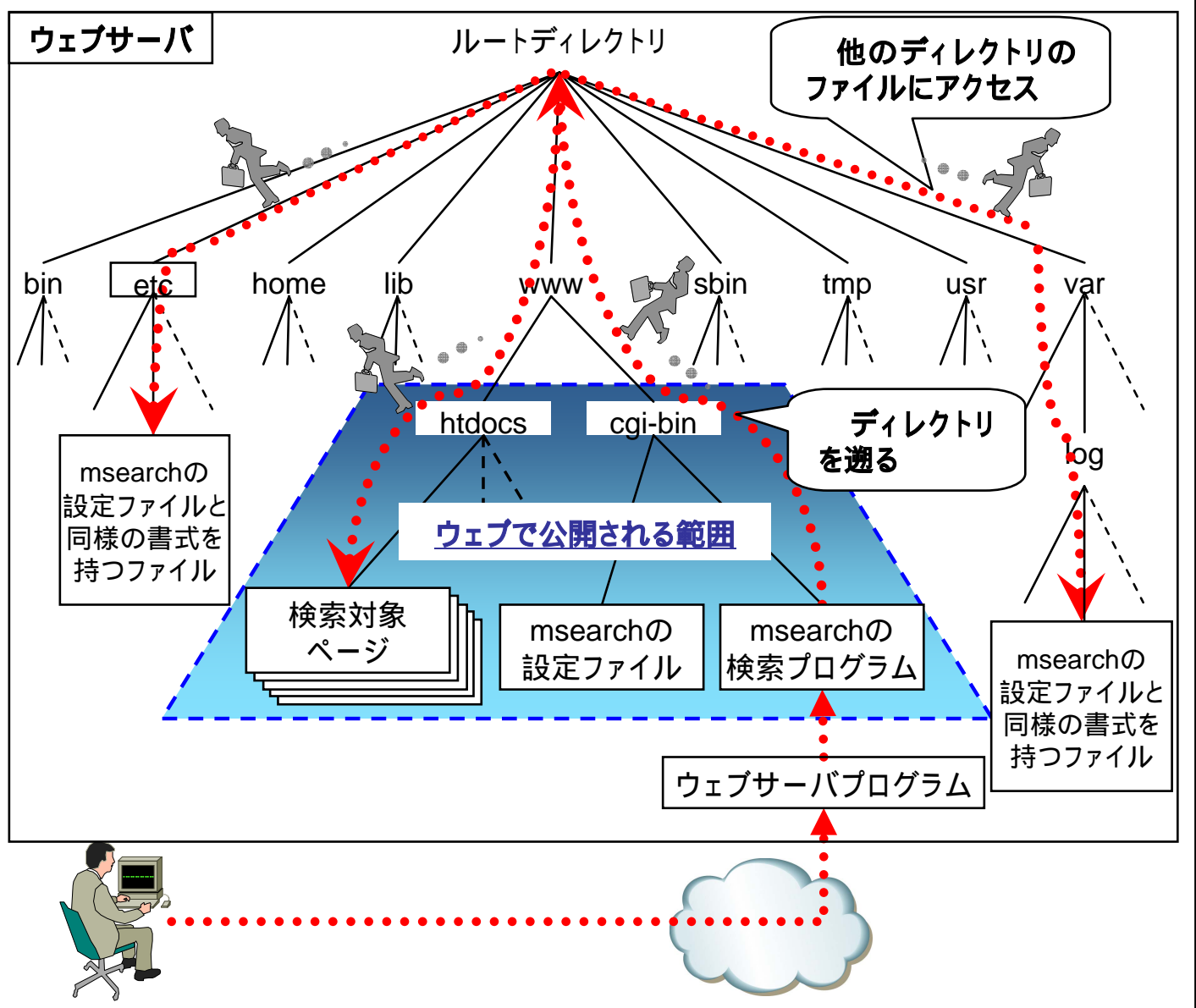
msearch は、ホームページ内の検索機能を提供する CGI プログラムです。msearch ver. 1.51 以前には、特定のファイルを開覧できてしまう問題があります。

悪意のある人は、msearch の検索機能を利用して、ウェブサーバ上に存在する全てのファイルにアクセスを試み、msearch の設定ファイルと同じ書式で記述されたファイルを、CGI の権限で閲覧することができます。

### msearch におけるディレクトリトラバーサル脆弱性の脆弱性

問題

設定ファイルと同じ書式のファイルを CGI の権限で閲覧できる



対象製品

msearch ver. 1.51 およびそれ以前

対策

msearch ver. 1.52 にアップデートしてください。  
詳しい製品情報については、製品開発者のサイト "きてーや.ねっと" (<http://www.kiteya.net/script/msearch/index.html>) を参照してください。

影響

他のディレクトリに存在する msearch の設定ファイル、インデックスファイル、これらのファイルと同様の書式を持つファイルの内容が漏洩する可能性があります。

脅威

設定ファイルが開覧されても、直接的な攻撃にはつながりません。

## 本脆弱性の深刻度:

### (1)評価結果

本脆弱性の <u>深刻度</u>	I(注意)	II(警告)	III(危険)
本脆弱性の <u>CVSS</u> 基本値		5.0	

### (2)CVSS 基本値の評価内容

AV: <u>攻撃元区分</u>	ローカル	隣接	ネットワーク
AC: <u>攻撃条件の複雑さ</u>	高	中	低
Au: <u>攻撃前の認証要否</u>	複数	単一	不要
C: <u>機密性への影響</u> (情報漏えいの可能性)	なし	部分的	全面的
I: <u>完全性への影響</u> (情報改ざんの可能性)	なし	部分的	全面的
A: <u>可用性への影響</u> (業務停止の可能性)	なし	部分的	全面的

注)・ : 選択した評価結果

・AV:AccessVector, AC:AccessComplexity, Au:Authentication,

C:ConfidentialityImpact, I:IntegrityImpact, A:AvailabilityImpact

### (3)注意事項

深刻度が低くても、対策をしなくてよいということではありません。

本ソフトウェアの利用者は必ず脆弱性対策を実施して下さい。