tenable | Plugins

Nessus

AjaXplorer checkInstall.php Arbitrary Command Injection

HIGH Nessus Plugin ID 45489

Information | Dependencies | Dependents | Changelog

Synopsis

The remote web application has an arbitrary command injection vulnerability.

Description

The version of AjaXplorer running on the remote web server has a command injection vulnerability. Input passed to the 'destServer' parameter of 'checkInstall.php' is used in a call to popen() without being properly sanitized.

A remote, unauthenticated attacker could exploit this to execute arbitrary commands on the system subject to the privileges of the web server user.

This version of AjaXplorer likely has other vulnerabilities, though Nessus has not checked for those issues.

Solution

Upgrade to AjaXplorer version 2.6 / 2.7.1 or later.

See Also

http://www.nessus.org/u?e68820e7

Plugin Details

Severity: High

ID: 45489

File Name: ajaxplorer_checkinstall_cmd_injection.nasl

Version: 1.24

Type: remote

Family: CGI abuses

Published: 4/12/2010

Updated: 9/29/2025

Configuration: Enable thorough checks (optional)

Supported Sensors: Nessus

Vulnerability Information

Required KB Items: www/ajaxplorer

Excluded KB Items: Settings/disable_cgi_scanning

Exploit Ease: No known exploits are available

Exploited by Nessus: true

Patch Publication Date: 4/4/2010

Vulnerability Publication Date: 4/4/2010

Exploitable With

Metasploit (AjaXplorer checkInstall.php Remote Command Execution)

Elliot (AjaXplorer 2.5.5 RCE (Windows))

Reference Information

BID: 39334

Documentation

Education