Vulnerability Report

Generated on: 2025-07-10 01:37

IP	192.168.1.10
Service	Apache HTTP Server
Version	2.4.29
CVE ID	CVE-2019-0211
Severity	HIGH
CVSS Score	7.8
Published	2019-03-01
CPE	cpe:2.3:a:apache:http_server:2.4.29:*:*:*:*:*:*:*

Summary

Risk: The CVE-2019-0211 vulnerability in Apache HTTP Server 2.4.29 has a high severity rating with a CVSS score of 7.8. This indicates a significant risk that could potentially allow unauthorized disclosure of information, unauthorized modification, or disrupted service. Affected Users: All users running the Apache HTTP Server version 2.4.29 are at risk. Remediation Steps: Users should immediately upgrade to the latest version of Apache HTTP Server. If an upgrade is not possible, users should apply the appropriate patch for CVE-2019-0211. It is also recommended to regularly check for updates and patches to prevent future vulnerabilities.

Risk

Risk: The CVE-2019-0211 vulnerability in Apache HTTP Server 2.4.29 has a high severity rating with a CVSS score of 7.8. This indicates a significant risk that could potentially allow unauthorized disclosure of information, unauthorized modification, or disrupted service.

Affected

All users of Apache HTTP Server version 2.4.29.

Remediation

Upgrade Apache HTTP Server to version 2.4.41 or later.