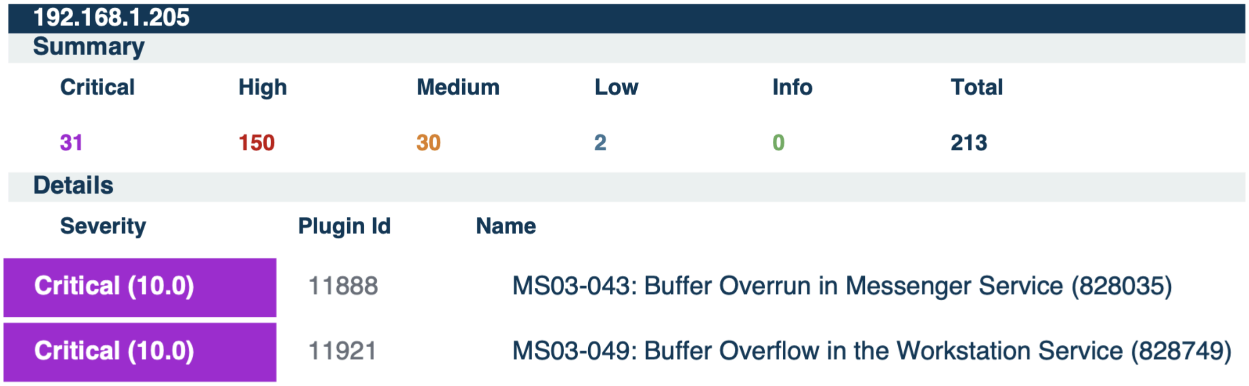
Vulnerability Scan Risk Assessment and Management Plan

I. Identification of Risks

Vulnerability Scan Results:



192.168.1.205

Summary

Critical	High	Medium	Low	Info	Total
31	150	30	2	0	213

Details

Severity	Plugin Id	Name
Critical (10.0)	11888	MS03-043: Buffer Overrun in Messenger Service (828035)
Critical (10.0)	11921	MS03-049: Buffer Overflow in the Workstation Service (828749)

Summary of Vulnerability Scan Results

- IP Address: 192.168.1.205
- Total Vulnerabilities: 213
    - Critical: 31
    - High: 150
    - Medium: 30
    - Low: 2
    - Informational: 0

Critical Vulnerabilities Identified:

1. **MS03-043: Buffer Overrun in Messenger Service (828035)**
    - Severity: Critical
    - Description: A buffer overrun vulnerability in the Windows Messenger Service could allow an attacker to execute arbitrary code on the target system.
2. **MS03-049: Buffer Overflow in the Workstation Service (828749)**
    - Severity: Critical
    - Description: A buffer overflow in the Workstation Service allows for remote code execution, enabling an attacker to gain complete control over the affected system.

II. Treatment Recommendations for Critical Risks

1. **MS03-043: Buffer Overrun in Messenger Service (828035)**
    - **Recommendation:** Apply the official Microsoft patch (MS03-043).

    - **Justification:** This vulnerability allows for remote code execution, potentially leading to full system compromise. Timely patching eliminates the risk.
    - **Mitigation Steps:**
        1. Download the security patch from Microsoft’s official site.
        2. Test the patch in a staging environment to ensure compatibility.
        3. Deploy the patch across all vulnerable systems.
        4. Disable the Messenger Service if not required.
2. **MS03-049: Buffer Overflow in the Workstation Service (828749)**
    - **Recommendation:** Apply the official Microsoft patch (MS03-049).
    - **Justification:** This vulnerability provides an attacker with the ability to execute arbitrary commands and take complete control over the system. Rapid remediation is essential.
    - **Mitigation Steps:**
        1. Obtain the security patch from Microsoft’s official site.
        2. Conduct testing in a controlled environment to identify any potential issues.
        3. Roll out the patch to all impacted devices.
        4. Regularly audit services and disable unnecessary ones to reduce attack surfaces.

III. Risk Monitoring Procedure: Scheduled Scans

Steps:

1. **Set Up Regular Scans:**
    - Schedule vulnerability scans on a weekly basis for critical assets and monthly for non-critical assets.
    - Use industry-standard tools like Nessus for scanning.
2. **Generate Reports:**
    - After each scan, generate a detailed report summarizing vulnerabilities and their severities.
3. **Track Progress:**
    - Maintain a log of vulnerabilities identified in each scan.
    - Assign remediation tasks to responsible teams with due dates.
    - Update the dashboard with patch deployment statuses and confirm resolution.
4. **Review and Verify:**
    - Conduct a review of resolved vulnerabilities to confirm that the fixes are effective.
    - Use follow-up scans to verify that no issues remain.

Regular scans and progress tracking ensure that vulnerabilities are continuously identified and remediated. This approach minimizes the likelihood of exploitation.