PRIVILEGE ESCALATION SECURITY REPORT

Report Type:	**Executive Summary**
Generated By:	**analyst**
Generation Date:	**2025-11-10 19:15:03**
Time Period:	**Last 30 days**

CONFIDENTIAL
This report contains sensitive security information. Distribution should be limited to authorized personnel only.

EXECUTIVE SUMMARY

This security assessment identified **1240** potential privilege escalation vectors across the monitored systems. Among these, **8** were classified as critical and **286** as high risk, requiring immediate attention. The analysis employed advanced detection methodologies including AI-powered pattern recognition and comprehensive system scanning to identify both known and emerging threats. **Key Recommendations:** • Prioritize mitigation of critical and high-risk findings • Implement continuous monitoring for privilege escalation attempts • Regular security awareness training for users • Periodic review of system permissions and access controls

DETAILED FINDINGS

1. Token Integrity Level Check - MEDIUM

Description:	Verify process token integrity levels manually
Category:	token_manipulation
CVSS Score:	5.5
Evidence:	Manual verification required for token integrity levels...
Mitigation:	Ensure processes run with appropriate integrity levels

2. Unquoted Service Path: Appinfo - MEDIUM

Description:	Service Appinfo has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: Appinfo TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 3 DEMAND_START ERROR_CONTROL : 1 NORMAL ...
Mitigation:	Add quotes to service path for Appinfo

3. Unquoted Service Path: AppXSvc - MEDIUM

Description:	Service AppXSvc has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: AppXSvc TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 3 DEMAND_START ERROR_CONTROL : 1 NORMAL ...
Mitigation:	Add quotes to service path for AppXSvc

4. Unquoted Service Path: AudioEndpointBuilder - MEDIUM

Description:	Service AudioEndpointBuilder has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: AudioEndpointBuilder TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 2 AUTO_START ERROR_CONTROL : 1 N...
Mitigation:	Add quotes to service path for AudioEndpointBuilder

5. Unquoted Service Path: Audiosrv - MEDIUM

Description:	Service Audiosrv has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0

Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: Audiosrv TYPE : 10 WIN32_OWN_PROCESS START_TYPE : 2 AUTO_START ERROR_CONTROL : 1 NORMAL ...
Mitigation:	Add quotes to service path for Audiosrv

6. Unquoted Service Path: BFE - MEDIUM

Description:	Service BFE has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: BFE TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 2 AUTO_START ERROR_CONTROL : 1 NORMAL BIN...
Mitigation:	Add quotes to service path for BFE

7. Unquoted Service Path: BrokerInfrastructure - MEDIUM

Description:	Service BrokerInfrastructure has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: BrokerInfrastructure TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 2 AUTO_START ERROR_CONTROL : 1 N...
Mitigation:	Add quotes to service path for BrokerInfrastructure

8. Unquoted Service Path: BTAGService - MEDIUM

Description:	Service BTAGService has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0

Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: BTAGService TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 3 DEMAND_START ERROR_CONTROL : 1 NORMAL ...
Mitigation:	Add quotes to service path for BTAGService

9. Unquoted Service Path: BthAvctpSvc - MEDIUM

Description:	Service BthAvctpSvc has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: BthAvctpSvc TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 3 DEMAND_START ERROR_CONTROL : 1 NORMAL ...
Mitigation:	Add quotes to service path for BthAvctpSvc

10. Unquoted Service Path: bthserv - MEDIUM

Description:	Service bthserv has unquoted path vulnerability
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	[SC] QueryServiceConfig SUCCESS SERVICE_NAME: bthserv TYPE : 20 WIN32_SHARE_PROCESS START_TYPE : 3 DEMAND_START ERROR_CONTROL : 1 NORMAL ...
Mitigation:	Add quotes to service path for bthserv

11. Unquoted Service Path: ADPSvc - MEDIUM

Description:	Service ADPSvc has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p

12. Unquoted Service Path: AppIDSvc - MEDIUM

Description:	Service AppIDSvc has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p"

13. Unquoted Service Path: Appinfo - MEDIUM

Description:	Service Appinfo has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k netsvcs -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k netsvcs -p"

14. Unquoted Service Path: AppMgmt - MEDIUM

Description:	Service AppMgmt has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k netsvcs -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k netsvcs -p"

15. Unquoted Service Path: AppReadiness - MEDIUM

Description:	Service AppReadiness has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\System32\svchost.exe -k AppReadiness -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\System32\svchost.exe -k AppReadiness -p"

16. Unquoted Service Path: AppXSvc - MEDIUM

Description:	Service AppXSvc has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k wsappx -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k wsappx -p"

17. Unquoted Service Path: ApxSvc - MEDIUM

Description:	Service ApxSvc has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k LocalService -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k LocalService -p"

18. Unquoted Service Path: AssignedAccessManagerSvc - MEDIUM

Description:	Service AssignedAccessManagerSvc has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\system32\svchost.exe -k AssignedAccessManagerSvc...
Mitigation:	Add quotes to service path: "C:\WINDOWS\system32\svchost.exe -k AssignedAccessManagerSvc"

19. Unquoted Service Path: AudioEndpointBuilder - MEDIUM

Description:	Service AudioEndpointBuilder has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p"

20. Unquoted Service Path: Audiosrv - MEDIUM

Description:	Service Audiosrv has unquoted path with spaces
Category:	service_vulnerability
CVSS Score:	5.0
Evidence:	Path: C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p...
Mitigation:	Add quotes to service path: "C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p"

MITIGATION RECOMMENDATIONS

- Implement principle of least privilege for all user accounts
- Regularly review and update system permissions
- Enable and monitor audit logs for privilege escalation attempts
- Apply security patches and updates promptly
- Conduct regular security awareness training
- Implement application whitelisting where appropriate
- Use security tools like Privileged Rapper Inc. for continuous monitoring