Layer Seven Security

ADVISORY

SAP Security Notes

November 2013

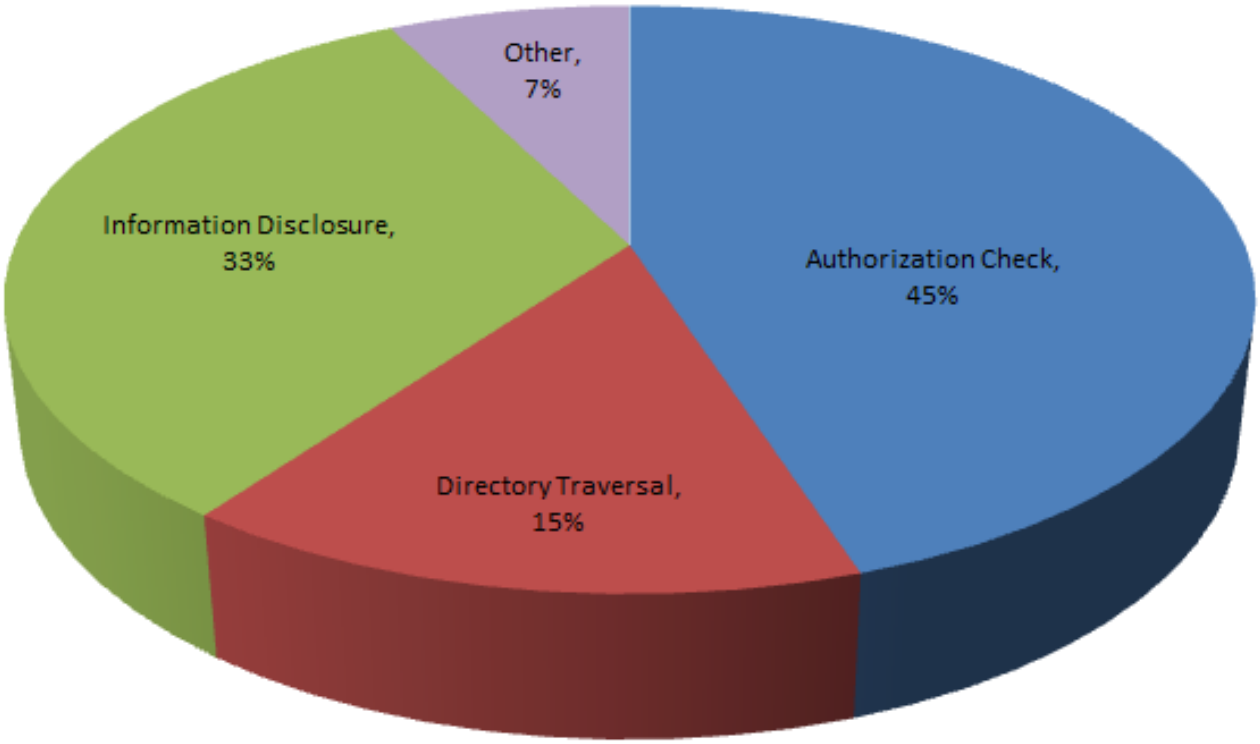
SAP Security Notes

November 2013

SAP issued a critical bulletin in November to raise awareness of three Security Notes related to SAProuter and a new malware variant that is currently under investigation. The SAProuter performs a pivotal role in SAP landscapes by controlling connections to backend systems from untrusted networks. Therefore, it is often targeted by malicious attackers. Misconfigurations in the component may enable attackers to discover SAP systems through the use of administrative commands. Options –I and –L for example, can be used to display route information from the permission table including connected clients and the corresponding IP addresses. The command –H will display route information to remote hosts. Other commands such as –S, –n and –X can be abused to change default ports, update route permission tables and control the SAProuter from external hosts. Such attacks can be mitigated by avoiding rules that inadvertently enable connections from unauthorized destinations and regularly updating the SAProuter with the latest release.

The first of the Notes cited by SAP in the bulletin relates to a buffer overflow vulnerability that could lead to the complete compromise of SAProuter (Note 1820666). The second and third carry a lower CVSS base score and contend with the risks associated with administrative commands that may be exploited by external attackers to discover information relating to network connections or change the configuration of the SAProuter (Notes 1663732 and 1853140).

Note 1903756 patches a missing authorization check that enables users to perform operating system (OS) commands through the DBA Cockpit used to monitor and administer SAP databases. The vulnerability affects IBM DB2/DB6 databases operating with both UNIX and NT servers. The ability of users to execute OS commands, also referred to as external commands, through the SAP layer should be



SAP Security Notes by Vulnerability Type

be tightly controlled through authorization objects such as S_LOG_COM and limited to specific commands, operating systems and hosts. The use of the object S_LOGCOM_ALL, which enables the execution of all external commands should be avoided, wherever possible. The correction instructions for Note 1903756 include the use of authorization S_ADMI_FCD with the appropriate field values to control external commands from the DBA Cockpit.

Note 1854408 deals with a vulnerability in GRC Access Request (ARQ) 10.0 and 10.1 that could lead to the disclosure of usernames and passwords in error messages generated by the application. Step 1 of the correction instruction represents a significant change to the password provisioning mechanism and therefore should only be implemented after extensive regression testing.

Finally, while there is no indication that the vulnerability addressed by Note 1677912 impacts Primary Account Numbers (PAN) for credit cards used by Payment Card Processing (SD-BIL-IV), the implementation of the objects included in the correction instructions is recommended since the vulnerability could lead to disclosure of personally identifiable information and expiry dates.

Appendix: SAP Security Notes, November 2013 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
2	1902611	BC-SEC	Potential information disclosure relating to BC-SEC
2	1903266	SRM-EBP-WFL	ABAP: Security issue with SRM offline approval
2	1903756	BC-DB-DB6-CCM	DB6: Authorization for executing operating system commands
2	1907712	PP-SFC-EXE	Missing authorization check in PP-SFC-EXE
2	1909230	BC-SRV-KPR	Missing authentication check in BC-SRV-KPR-CMS
2	1909442	IS-M-SD-PS-SL-O	Incorrect authorization check in IAC post processing
2	1909665	CA-WUI-UI-TAG	Untrusted XML input parsing possible in CA-WUI-UI-TAG
2	1910737	LO-SCI-POI	Missing authorization check in LO-SCI-POI
2	1912377	CRM-ISA	Potential information disclosure relating to CRM-ISA
2	1916550	BC-DWB-CEX	Missing authorization check in BAdI Framework
2	1812543	BC-WD-ABA	Missing authorization check in Web Dynpro ABAP
2	1836314	BC-MID-RFC	Missing authorization check for calling transactions
2	1846945	EPM-BPC-NW	Missing authorization check in BPC Web & Web Administration
2	1853140	BC-CST-NI	Managing SAProuter from external host
2	1854408	GRC-SAC-ARQ	Potential information disclosure relating to user password
2	1864518	MOB-APP-EMR-AND	Security Improvements for MOB-APP-EMR-AND
2	1881062	FI-GL-GL-G	Missing authorization check in FI-GL-GL-G
2	1881374	IS-A-SWP	Missing authorization check in IS-A-SWP.
2	1884212	FI-BL-PT-BA	Bank statement: Potential directory traversal
3	1794951	XX-CSC-BR	Directory traversal in XX-CSC-BR
3	1775843	IS-H-PM	Directory traversal in IS-H in utilities (reports)
3	1916257	PA-PA-US	Directory traversal in PA-PA-US
3	1898735	BC-CCM-MON	Directory traversal in standalone CCMS agents
3	1899146	BC-XI-IS	Potential disclosure of information about PI

Appendix: SAP Security Notes, November 2013 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
3	1900036	CRM-ISA	Potential information disclosure relating to CRM-ISA
3	1902402	CRM-FM-ACL	Missing whitelist check in CRM-FM-ACL
3	1902986	CRM-FM-ACL	Missing whitelist check in CRM-FM-ACL
3	1905591	CRM-MD-BP-IF	Missing authorization check in CRM business partner
3	1906568	CRM-MW-ADP	Missing authorization check in CRM-MW-ADP functions
3	1677912	SD-BIL-IV-PC	Credit cards in order
3	1786150	CRM-MD-BP	Potential disclosure of persisted data in [crm-md-bp]
3	1813155	EHS-BD	Possible change/disclosure of persisted data in EH&S
3	1836718	BW-WHM-DBA-IOBJ	Potential disclosure of persisted data in BW-WHM-DBA-IOBJ
3	1843169	CRM-MW-ADP	Missing authorization check in CRM-MW-ADP
3	1861907	CRM-ISA-TEC	Potential information disclosure relating to CRM-ISA-TEC
3	1922205	BC-XI-IS-WKB	Berechtigungsvorschlag in Komponente BC-XI-IS-WKB
3	1735308	BC-CUS-TOL-ALO	Security issues for report TAB_INTO_AUTH_GRP
3	1787032	FI-AP-AP-B1	FI: Potential Directory Traversal
4	1897192	BC-JAS-SEC-UME	Password hash algorithm in UME
4	1788562	LO-LIS-REP	Potential modif./disclosure of persisted data in LO-LIS-REP

LAYER SEVEN SECURITY

Layer Seven Security empowers organisations to realize the potential of SAP systems. We serve customers worldwide to secure systems from cyber threats. We take an integrated approach to build layered controls for defense in depth

Address
Westbury Corporate Centre
Suite 101
2275 Upper Middle Road
Oakville, Ontario
L6H 0C3, Canada

Web
www.layersevensecurity.com
Email
info@layersevensecurity.com
Telephone
1 888 995 0993