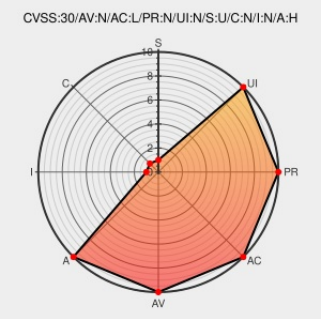
CVE-2017-14511

Published on: 09/17/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14511

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of E-recruiting from Sap contain the following vulnerability:

An issue was discovered in SAP E-Recruiting (aka ERECRUIT) 605 through 617. When an external applicant registers to the E-Recruiting application, he/she receives a link by email to confirm access to the provided email address. However, this measure can be bypassed and attackers can register and confirm email addresses that they do not have access to (candidate_hrobject is predictable and corr_act_guid is improperly validated). Furthermore, since an email address can be registered only once, an attacker could prevent other legitimate users from registering. This is SAP Security Note 2507798.

CVE-2017-14511 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link

Email verification bypass in SAP E-Recruiting – SEC Consult	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.sec-consult.com/en/blog/advisories/email-verification-bypass-in-sap-e-recruiting/index.html
No Description Provided	Permissions Required Vendor Advisory launchpad.support.sap.com text/html	MISC launchpad.support.sap.com/#/notes/2507798
SAP Security Patch Day – September 2017 | SAP Blogs	Vendor Advisory blogs.sap.com text/html	MISC blogs.sap.com/2017/09/12/sap-security-patch-day-september-2017/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	E-recruiting	605	All	All	All
Application	Sap	E-recruiting	606	All	All	All
Application	Sap	E-recruiting	616	All	All	All
Application	Sap	E-recruiting	617	All	All	All
Application	Sap	E-recruiting	605	All	All	All
Application	Sap	E-recruiting	606	All	All	All
Application	Sap	E-recruiting	616	All	All	All
Application	Sap	E-recruiting	617	All	All	All

cpe:2.3:a:sap:e-recruiting:605:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:606:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:616:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:617:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:605:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:606:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:616:*:*:*:*:*:*:*:*

cpe:2.3:a:sap:e-recruiting:617:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→