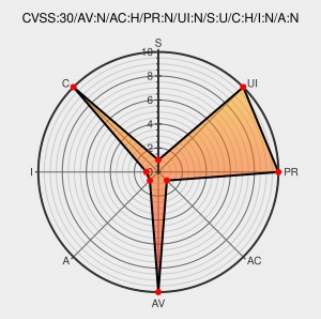
CVE-2014-10067

Published on: 05/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-10067

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



Certain versions of Paypal-ipn from Paypal-ipn Project contain the following vulnerability:

paypal-ipn before 3.0.0 uses the `test_ipn` parameter (which is set by the PayPal IPN simulator) to determine if it should use the production PayPal site or the sandbox. With a bit of time, an attacker could craft a request using the simulator that would fool any application which does not explicitly check for test_ipn in production.

CVE-2014-10067 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **HackerOne** - **paypal-ipn node module** version **<3.0.0**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Overview	Third Party Advisory	MISC nodesecurity.io/advisories/26

web.archive.org
text/html
Inactive Link Not Archived

Issue Tracking
Third Party Advisory
github.com
text/plain
Inactive Link Not Archived

MISC github.com/andzdroid/paypal-ipn/issues/11

Related QID Numbers

980713 Nodejs (npm) Security Update for paypal-ipn (GHSA-h698-r4hm-w94p)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paypal-ipn Project	Paypal-ipn	All	All	All	All
Application	Paypal-ipn Project	Paypal-ipn	All	All	All	All

cpe:2.3:a:paypal-ipn_project:paypal-ipn:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:paypal-ipn_project:paypal-ipn:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→