



CVE-2013-4114

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-4114
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-16 17:55:05 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The automatic update request in Nagstamon before 0.9.10 uses a cleartext base64 format for transmission of a username

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-255 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Henri Wahl	Nagstamon	0.5.10	All	All	All

Application	Henri Wahl	Nagstamon	0.5.11	All	All	All
Application	Henri Wahl	Nagstamon	0.5.13	All	All	All
Application	Henri Wahl	Nagstamon	0.5.2	All	All	All
Application	Henri Wahl	Nagstamon	0.5.3	All	All	All
Application	Henri Wahl	Nagstamon	0.5.4	All	All	All
Application	Henri Wahl	Nagstamon	0.5.5	All	All	All
Application	Henri Wahl	Nagstamon	0.5.6	All	All	All
Application	Henri Wahl	Nagstamon	0.5.7	All	All	All
Application	Henri Wahl	Nagstamon	0.5.8	All	All	All
Application	Henri Wahl	Nagstamon	0.5.9	All	All	All
Application	Henri Wahl	Nagstamon	0.6	All	All	All
Application	Henri Wahl	Nagstamon	0.6.1	All	All	All
Application	Henri Wahl	Nagstamon	0.6.2	All	All	All
Application	Henri Wahl	Nagstamon	0.7.0	All	All	All
Application	Henri Wahl	Nagstamon	0.8.0	All	All	All
Application	Henri Wahl	Nagstamon	0.8.1	All	All	All
Application	Henri Wahl	Nagstamon	0.8.2	All	All	All
Application	Henri Wahl	Nagstamon	0.9.0	All	All	All
Application	Henri Wahl	Nagstamon	0.9.1	All	All	All
Application	Henri Wahl	Nagstamon	0.9.2	All	All	All
Application	Henri Wahl	Nagstamon	0.9.3	All	All	All
Application	Henri Wahl	Nagstamon	0.9.4	All	All	All
Application	Henri Wahl	Nagstamon	0.9.5	All	All	All
Application	Henri Wahl	Nagstamon	0.9.6	All	All	All
Application	Henri Wahl	Nagstamon	0.9.6.1	All	All	All
Application	Henri Wahl	Nagstamon	0.9.7	All	All	All
Application	Henri Wahl	Nagstamon	0.9.7.1	All	All	All
Application	Henri Wahl	Nagstamon	0.9.8	All	All	All
Application	Henri Wahl	Nagstamon	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
089672 (CVE-2019-1114) CVE-2019-1114 nagstamon: Monitor server user credentials exposure in automated requests to get update inform

983673 - (CVE-2013-4114) CVE-2013-4114 nagstamon: monitor server user credentials exposure in automated requests to get update info

Nagstamon :: Security

Security Advisory SA54072 - Nagstamon Login Credentials Disclosure Security Issue - Secunia

476538 - (CVE-2013-4114) <net-analyzer/nagstamon-0.9.11_rc1: User credentials exposure (CVE-2013-4114)

openSUSE-SU-2013:1235-1: moderate: update for nagstamon

About Secunia Research | Flexera

oss-security - Re: CVE Request -- Nagstamon (prior 0.9.10): Monitor server user credentials exposure in automated requests to get update inf

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.
CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).
Free CVE JSON API [cve.report/api](#)
CVE.report and Source URL Uptime Status [status.cve.report](#)