



CVE-2018-12356

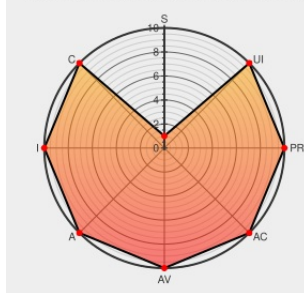
Published on: 06/14/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:23 PM UTC

CVE-2018-12356

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Simple Password Store](#) from [Simple Password Store Project](#) contain the following vulnerability:

An issue was discovered in password-store.sh in pass in Simple Password Store 1.7.x before 1.7.2. The signature verification routine parses the output of GnuPG with an incomplete regular expression, which allows remote attackers to spoof file signatures on configuration files and extension scripts. Modifying the configuration file allows the attacker to inject additional encryption keys under their control, thereby disclosing passwords to the attacker. Modifying the extension scripts allows the attacker arbitrary code execution.

CVE-2018-12356 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Johnny You Are Fired/johnny-fired.pdf at master · DUP	CVE-2018-12356	MISC github.com/DUP-NDS/johnny-you-are-fired

Johnny-You-Are-Fired/johnny-fired.pdf at master · RUB-NDS/Johnny-You-Are-Fired · GitHub	github.com text/html	MISC github.com/RUB-NDS/Johnny-You-Are-Fired/blob/master/paper/johnny-fired.pdf
password-store - Simple password manager using gpg and ordinary unix directories.	Patch Third Party Advisory git.zx2c4.com text/html	MISC git.zx2c4.com/password-store/commit?id=8683403b77f59c56fcb1f05c61ab33b9fd61a30d
GitHub - RUB-NDS/Johnny-You-Are-Fired: Artifacts for the USENIX publication.	github.com text/html	MISC github.com/RUB-NDS/Johnny-You-Are-Fired
oss-security - Spoofing OpenPGP and S/MIME Signatures in Emails (multiple clients)	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20190430 Spoofing OpenPGP and S/MIME Signatures in Emails (multiple clients)
oss-security - CVE-2018-12356 Breaking signature verification in pass (Simple Password Store)	Mailing List Third Party Advisory openwall.com text/html	MISC openwall.com/lists/oss-security/2018/06/14/3
Johnny You Are Fired ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152703/Johnny-You-Are-Fired.html
Security Vulnerability: Faulty GPG Signature Checking	Mailing List Third Party Advisory lists.zx2c4.com text/html	MISC lists.zx2c4.com/pipermail/password-store/2018-June/003308.html
Full Disclosure: OpenPGP and S/MIME signature forgery attacks in multiple email clients	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20190430 OpenPGP and S/MIME signature forgery attacks in multiple email clients

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple Password Store Project	Simple Password Store	All	All	All	All
Application	Simple Password Store Project	Simple Password Store	All	All	All	All
cpe:2.3:a:simple_password_store_project:simple_password_store:*****:						
cpe:2.3:a:simple_password_store_project:simple_password_store:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)