# CVE Detail – CVE-2006-1058

BusyBox 1.1.1 does not use a salt when generating passwords, which makes it easier for local users to guess passwords from a stolen password file using techniques such as rainbow tables.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.13507

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-916: Use of Password Hash With Insufficient Computational Effort

## CAPEC(s)

* CAPEC-55: Rainbow Table Password Cracking

## ATT&CK Techniques

* T1110.002: Password Cracking

## Used By (Actors/Tools)

* Net Crawler (malware)
* Dragonfly (intrusion-set)
* FIN6 (intrusion-set)
* Night Dragon (campaign)
* Salt Typhoon (intrusion-set)
* APT3 (intrusion-set)

## Affected Products

* cpe:2.3:a:busybox:busybox:1.1.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:avaya:aura\_application\_enablement\_services:4.01:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:avaya:aura\_application\_enablement\_services:4.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:avaya:aura\_sip\_enablement\_services:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:avaya:message\_networking:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:avaya:messaging\_storage\_server:\*:\*:\*:\*:\*:\*:\*:\*