Missing HTTP Strict Transport Security (HSTS) Protection

By having HTTP to HTTPS redirects, the attackers can "strip" SSL from a session. The attackers need to be on the same network for this to work. So, think coffee shops... evil, coffee shops.

DETECTION

Firewall Log Review
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

SSLStrip
SSLSplit

https://github.com/droe/sslsplit

https://github.com/moxie0/sslstrip

Backdoors™ & Breaches

INITIAL COMPROMISE

Created by: BLACK HILLS | Information Security