

19 August 2009

By: Catalin Cimpanu, Web News Editor

[Pidgin Vulnerability Fixed with Latest Releases](#)

CORESecurity and Pidgin quietly fix malware vulnerability



Pidgin vulnerability fixed through the release of the 2.5.9 version
The Pidgin Team

CORESecurity recently [discovered](#) and quietly informed Pidgin developers of a security [vulnerability](#) inside the main Pidgin core library that would have permitted third parties to remotely execute malware on a computer. Through the latest releases of the Pidgin instant messaging software, the vulnerability was successfully fixed.

The CORESecurity team discovered that, by sending specially formatted MSNSLP messages to a Pidgin client through a MSN server, it might be possible to crash a remote computer. The consecutive messages were triggering a memcpy action in the system's memory, resulting in an invalid memory allocation that crashed the PC.

This vulnerability does not require any user interaction, nor for the attacker to be in the victim's buddy list.

Vulnerable was the base core library of the Pidgin client, called Libpurple. The same library powers many other IM clients like Apollo, EQO, Instantbird, Meebo, Palm and Telepathy-Haze.

The above-mentioned library affects only Gaim 0.79 or higher, Pidgin releases until 2.5.9, Finch and Adium 1.5.8 or sooner. CORESecurity quietly informed the Pidgin team about this security problem, and waited until a patched version (2.5.9) was released before making it public.

Meanwhile, the Pidgin team released two new versions, 2.6.0 and 2.6.1, incorporating even better fixes for the Libpurple [vulnerability](#). On Pidgin's main site, the latest download available Windows binaries still remain the ones from the 2.5.8 version, the version on which the hack was initially tested and discovered.

For better protection, Pidgin users should download a patched version, CORESecurity recommending 2.6.0 as the version from which the [vulnerability](#) was completely fixed.

Regarding these incidents, John Bailey, Pidgin Team representative said that, "CORE Security Technologies found a way to remotely crash a running Pidgin instance that was logged into an MSN account via two specially crafted messages. They were kind and responsible enough to inform us of this privately and provide us with a proof of concept script so we could fix the problem before they made it public. The release of Pidgin 2.5.9 was done in source form only, explicitly to provide distribution packagers with a fixed release in the event they preferred to avoid the behemoth release that is 2.6.0."

Pidgin 2.6.1 sources (latest version) can be found [here](#).