

[NT] Halo Off-By-One Bug Can Crash Multiplayer Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/04

To: list@securiteam.com

Date: 14 Sep 2004 15:16:10 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Halo Off-By-One Bug Can Crash Multiplayer Server

SUMMARY

" <<http://www.bungie.net/Games/HaloPC/>> Halo for PC is a conversion of Bungie's Xbox classic – a first person sci-fi shooter set on a ring-shaped alien artifact in deep space, as you in the role of Master Chief, attempt to stop an alien race known as The Covenant from reaching Earth."

A bug in the way the server handles handshakes with a connecting client allows the client to crash the server if a malformed packet is sent.

DETAILS

Vulnerable Systems:

- * Halo: Combat Evolved, version 1.4 and prior (PC and Mac)

Immune Systems:

- *Halo: Combat Evolved, patch version 1.5 (PC and Mac)

Halo uses the Gamespy SDK and specifically, the handshake algorithm provided in this library to let players to join servers. A breakdown of the algorithm is given by Luigi at

Securiteam: [NT] Halo Off-By-One Bug Can Crash Multiplayer Server

<<http://aluigi.altervista.org/papers/gssdkcr.h>>
<http://aluigi.altervista.org/papers/gssdkcr.h>.

In the last stage of the handshake taking place between the server and the connecting client, the client is sending the last response. If this last response is longer than 32 bytes, it will immediately cause the Halo online server to crash.

A proof of concept code that demonstrates this can be downloaded from
<<http://aluigi.altervista.org/poc/haloboom.zip>>
<http://aluigi.altervista.org/poc/haloboom.zip>.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:aluigi@autistici.org>> Luigi Auriemma.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.