Do Enterprise Management Systems Dream Of Electric Sheep?

Thomas Ptacek

Dave Goldsmith
Who We Are

- Dave Goldsmith (@stake cofounder)
- Jeremy Rauch (SecurityFocus cofounder)
- Thomas Ptacek (Arbor)
- Window Snyder (Microsoft XPSP2)
- Dino Dai Zovi (Bloomberg)
What We Do

- **DEPLOYSAFE**
  Reverse and Pen-Test Products for enterprises
- **SHIPSAFE**
  Audit and Test Products for vendors
- **CLOCKWORK**
  our First Product coming July/August 2006
Project Chinashop

- First iSCSI Protocol Finding
- Broke Market-Leading D-R Product
- Broke CORBA
- Broke 3 Message Middleware Protocols
- First iFCP Protocol Finding
- Novell SAN Findings
- Broke Most of Agent Market
- 25+ Advisories Backlogged
Project Chinashop

• Example Finding:
  - on the market-leading iSCSI SAN server you can attach to targets without authenticating.
Today’s Target:
Enterprise Management Applications ("DSM")
What is DSM

- the stuff IT installs on every server and every desktop as part of the standard build
- provides:
  - central config management
  - central status reporting
  - central software update
  - central job scheduling
DSM In Perspective

• The Leading DSM Vendor *(for whom DSM is 40%+ of revenue)* booked over $1.4Bn ‘05.
• That’s The Same League as SYMC.
What DSM Looks Like

- Lots of Agents
- One Management Server
- Management Clients
What DSM Looks Like
What DSM Looks Like

- Lots of Agents
- One Management Server
- Management Clients

Bots

Command and Control

Attackers
Round 1: Server v. Agent

- Can Attacker Posing As Server Bust The Agent?
Round 2: Agent v. Server Listener

- Can Attacker Posing As Agent Bust The Server Directly?
Round 3: Agent v. Server Client

- Can Attacker-Controlled Agent Bust The Server In Response To A Query?
Round 4: Eve vs. Agent & Sever

- Can An Eavesdropper Recover Credentials From Management Connections?
Round 5:
OWASP v. Server

- Can An Attacker Control The Server via Flawed Web Interface?
Round 6: Agent v. Browser

- Can Responses Generated From Agents Inject Javascript Into Browsers?
Round 7: Client v. Server

- Can An Attacker Posing As A Windows Management Client Bust The Server?
Round 8: Server v. Client

- Can An Attacker Posing As A Management Component Bust The Windows Management Client?
Round 9: Agent v. Client

- What Will The Client Do If The Attacker’s Agent Generates A 10240-byte Status Response?
Round 10: Client v. Middleware

• Can An Attacker Take Out The Messaging Layer?
Round 11: Eve v. Client/Server

Can An Eavesdropper Recover Credentials From Windows Management Client Session?
Round 12: Client v. Database

- Does The Default Install Lock Down The Database?
Wrinkles

- Some Management Systems Have More Than One Windows Client
- Some Have More Than One Messaging Layer
CORBA
Stop Laughing. This Stuff Controls The Cooling Rods.
## CORBA Decoder Ring

<table>
<thead>
<tr>
<th>corba</th>
<th>web</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOP</td>
<td>HTTP</td>
</tr>
<tr>
<td>Message</td>
<td>POST</td>
</tr>
<tr>
<td>ORB</td>
<td>Apache</td>
</tr>
<tr>
<td>Object</td>
<td>Page</td>
</tr>
<tr>
<td>IOR</td>
<td>URI</td>
</tr>
<tr>
<td>CosNaming</td>
<td>DNS</td>
</tr>
<tr>
<td>Method</td>
<td>&amp;action=</td>
</tr>
<tr>
<td>SvcContext</td>
<td>Cookie</td>
</tr>
<tr>
<td>MessageBody</td>
<td>POST Args</td>
</tr>
</tbody>
</table>
OMG Naming
matasano chargen
www.matasano.com/log
Clearly, we don’t believe in silence, neither should you.

tqbf@matasano.com
daveg@matasano.com