ESA-20180417-02
SmartServer Authentication Bypass Flaw

Overview

It is possible to bypass the required authentication specified in the security configuration file by including extra characters in the directory name when specifying the directory to be accessed. Echelon recommends that all SmartServers be installed behind a firewall or on a VLAN to minimize exposure to attackers.

Affected Products

All SmartServer 2 and SmartServer 1 products.

Vulnerability Overview

Authentication on the SmartServer is controlled by configuration directives in the **WebParams.dat** file. When specifying that a particular set of files or directories should be inaccessible without authentication, the path is placed in the configuration file as a string with optional wildcard characters (*) to match zero or more characters. When a Web request is made, the URI must match the entire provided path with wildcards applied, or no authentication will be required. By issuing Web requests with superfluous slashes in the URI (for example, "/forms/////Echelon/SetupSecurity.htm"), the path will not match the one configured to require authentication and will be accessible without any username or password.

Risk Evaluation

The risk is high for a SmartServer not installed behind a firewall or on a VLAN. The risk can be mitigated by installing the SmartServer behind a firewall or on a VLAN as described in the next section.

Mitigation

To minimize exposure to attackers, install the SmartServer and any servers using the SmartServer behind a firewall or on a VLAN without other devices. The VLAN approach limits the threat vector from other internal devices and users that are not part of the same system with the SmartServer and associated servers. When using a firewall, to minimize threat exposure do not configure the firewall to do any port forwarding to the SmartServer.

SmartServer 2.2 Service Pack SP7 addresses this Authentication Bypass Flaw and can be downloaded from the Echelon website.

Acknowledgement

Echelon thanks Daniel Crowley and IBM's X-Force Red team for reporting the vulnerabilities.

History

V1.0 (2018-04-17): Initial publication

V2.0 (2018-9-11): Removed i.LON 600 from bulletin (separate bulletin, ESA-20180823-01, published for i.LON 600) and added SmartServer Service Pack that addresses this security flaw

PGP Signature

To send an encrypted communication to Echelon concerning any security vulnerability questions, reports, or issues, use the following PGP key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFrCu+QBCADim1Dv1Xj+wYUMpniZM0J5Cv9VtBK95NrW3U956p6s6w/WAbBj
c52p4+qF01dmXMg6x14a8lMUDzJxfzW/at6U8HcZp+Kd8TBgmU9xLpZFcb3ey41z
KbcC39c3shL9JnERci5ObB8BHsbNAswhNn7wbpMkgLfLJltxyAYlNK7T9mepO3Rp
WnecyaKT21UWTE2vo1TEB1Jx6P5luCkIHeVVrZZlQmLHY4B6dU1VN4g9ngut/LNx
Rfnu9nfkwAV5sljW6zmmB6jRSgu+vV2s6rVoyc3ATxViAQDAMMOkSlOdU7gYSOSL
uXyR1bVgOTFhhPVQO+no55z/h/SfDupXqee1ABEBAAG0CFJpY2ggS2V5iQFOBBMB
CAA4FiEEFTDZ9piFJnflLx2IFAu2dl7bl7UFAlrCu+QCGwMFCwkIBwIGFQoJCAsC
BBYCAwECHgECF4AACgkQFAu2dl7bl7VeUAf+Ik9Cqx4Xhyg0P/0MFuvWd9ywqQgk
B3zIs+IyBwuwRQnUoWRfWGB/JWK4Ocfe7AjDzAbHcScMuCZniY/Bq1QpuguyeD9K
/d3YM17wkW2pwHkk1xd7yHIkl0g87Uedt4133YOBLU/eUeAVTFQ0QLaFLzbXICO7
h7S3vXsXTao5V2GPeY4AM1i/h3tMUeOXT0ASWCL9S7AQavKnGr8HJX1e+ikj8rVX
icRBA0xcg17aSqRUdyCFJi5W0AaKXDVJSWRz6hszF799PqS/syLqYxYSU+t1uHVd
7Qnq3gPnA+qUZuTzUTqZzMDccxW/MAeazjHik0XK4Nb7BGM8wBkhO8ZT4LkBDQRa
wrvkAQgAsvyLqmDZ+1jwslTUAWLS3sJQxAjtRywgSMxiUJgGDhGYvmOqagGrVmnD
LDS8WnplKtgPpgwKtUY1nIQeYwQ0wrFvkwVX7iokYKWrgBTaiJLVk3SqvGqhb4Nb
8wDLpj6TjOT2B/KqNaT8NS9WVj4VCjOm6eR2R+gM2njVDu3Gl1uLDwQm3VHbJUJG
JTybM0sSUtf/ZOefZkAE0tiCbgMaI7J1slCat9twU+yABLwmcFy/Fk5A+krHSLM2
k5YstWj9CBzTc+LgndTHJNK0fZk0plVG1Jar9+1TArbPEY7e6qlNlaT7BbL9/Dmd
XDyjvx9bP1Xmgk3hZBfzQmr7DvOGGQARAQABiQE2BBgBCAAgFiEEFTDZ9piFJnfl
Lx2IFAu2dl7bl7UFAlrCu+QCGwwACgkQFAu2dl7bl7WORAf/eFQ4TiW0KhxizvFk
Exmkdq3wYU7ymbX5KfCy+jhkhaF8UiR6We2jJ8Ko5ndR7zCy99H8lqSMNQTqCV27
Al/3iRTKXESqzoQdtjCoihtY/ZlqYUVaY2wsaj0mHzzARPXc4EXHxqhyBoqON7uf
U8b0Nxwk6646BpPwl1LqWSNScV2t0yXiJp62YzaGZZ1DN5rXWQL5yUI3O4fOWrfz
OkjbF4miRlXhmrm7dhs9mK9ctNZFYMQoqgacRj7/ASyjcYoSL1M2GXXXqE7IJyiB
C2oIzDaIPgJdurOKrEnWelCj7qIJq4gAfp+WIIFjdCgqgxPGL6O1GTygWetFEETK
UzV1yg==
=mgme
-----END PGP PUBLIC KEY BLOCK-----